

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-342518

(43)Date of publication of application : 29.11.2002

(51)Int.Cl. G06F 17/60

G06F 12/14

G06F 15/00

H04N 5/765

H04N 5/91

H04N 7/173

(21)Application number : 2002-024695 (71)Applicant : MATSUSHITA ELECTRIC
IND CO LTD

(22)Date of filing : 31.01.2002 (72)Inventor : AZUMA AKIO
MURAKAMI HIRONORI
MATSUO TAKASHI
NAKAHARA TORU
NANBA TAKAAKI
GOTO YOSHIMASA
NAKANISHI MASANORI
MIYAZAKI MASAYA
KOZUKA MASAYUKI

(30)Priority

Priority number : 2001027278

Priority date : 02.02.2001

Priority country : JP

(54) SYSTEM AND METHOD FOR CONTENTS USE MANAGEMENT

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a contents use management system, etc., which enables a server to surely and easily control the use of contents on a user terminal without placing any load on the user terminal.

SOLUTION: The server 100 of the contents use management system is equipped with a user right information DB 120 which stores right information regarding the right to use contents that the user using the user terminal 200a has and a contents information generation part 170 which generates LT as right information showing part of the use right that the user has at a request made by the user and sends it to the user terminal 200a. The user terminal 200a, on the other hand, is equipped with a communication part 210 which receives the LT sent from the server 100 and a license information processing part 260 which controls the use of the contents according to the use right that the received LT shows.

* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.*** shows the word which can not be translated.

3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1]A contents use management system which consists of a terminal unit using contents characterized by comprising the following which are digital works, and a server apparatus which manages use in said terminal unit of said contents via a transmission line.

A right-information-data memory measure which memorizes right information data about a utilization right of contents which a user for whom said server apparatus uses said terminal unit owns.

Based on a demand from said user, a license ticket which is right information data which show a part of utilization right which the user concerned owns is generated, A reception means which receives a license ticket which was provided with a license ticket issuing means which transmits to said terminal unit, and in which said terminal unit has been transmitted from said server apparatus.

A contents utilization control means to control use of said contents according to a utilization right which a received license ticket shows.

[Claim 2]The contents use management system according to claim 1, wherein said license ticket issuing means acquires a demand which specifies a part of utilization right which said user owns from the user concerned, generates a license ticket corresponding to the specification and transmits to said terminal unit.

[Claim 3]The contents use management system according to claim 1, wherein said license ticket issuing means generates a license ticket in which a utilization right of the minimum unit which constitutes a utilization right which said user owns is shown and transmits to said terminal unit.

[Claim 4]The contents use management system according to claim 1, wherein said license ticket consists of one or more propriety information about use of contents.

[Claim 5]The contents use management system according to claim 4, wherein said

propriety information shows propriety of either reproduction of contents, movement and a duplicate.

[Claim 6]The contents use management system according to claim 4 characterized by a thing of one use or more in which said propriety information contains an infinite time of contents, and for which good or a failure is shown.

[Claim 7]After enciphering said license ticket, said license ticket issuing means transmits to said terminal unit, and said terminal unit, Have a decoding means which decrypts a license ticket received by said reception means, and said contents utilization control means, The contents use management system according to claim 1 characterized by controlling use of said contents according to a utilization right which a decrypted license ticket shows.

[Claim 8]The contents use management system according to claim 7, wherein said decoding means and a contents utilization control means are the Tampa[-proof]-ized security modules.

[Claim 9]The contents use management system according to claim 1, wherein detection information for detecting whether the contents of the license ticket concerned were altered is included in said license ticket.

[Claim 10]The contents use management system according to claim 1 when it judges whether said license ticket permits use of further contents and does not approve [said contents utilization control means], after contents are used, wherein it cancels the license ticket concerned.

[Claim 11]Said terminal unit is provided with a still more nearly removable external recording medium, and said contents utilization control means, When a license ticket in which after a license ticket before contents are used, and contents use permits use of further contents permits movement of contents, The contents use management system according to claim 10 storing the license ticket in said external recording medium.

[Claim 12]Said external recording medium connected to said terminal unit further said terminal unit, Have a judging means which judges whether it has a means to control use of said contents according to a utilization right which said license ticket shows, and said contents utilization control means, The contents use management system according to claim 11 characterized by storing a license ticket in an external recording medium when judged with said external recording medium being provided with said control means.

[Claim 13]The contents use management system according to claim 12 changing said contents utilization control means into contents control information on a format which

is different in said license ticket when judged with said external recording medium not being provided with said control means.

[Claim 14]The contents use management system according to claim 6 characterized by said contents utilization control means judging use of contents based on said criteria to be 1 time including criteria used as a standard which use of contents judges that said propriety information was performed once.

[Claim 15]The contents use management system according to claim 14, wherein said criteria are set up according to a use mode of contents.

[Claim 16]The contents use management system according to claim 15 which said criteria are the time when contents were reproduced, and is characterized by said contents utilization control means judging use of contents based on said regeneration time of contents to be 1 time.

[Claim 17]The contents use management system according to claim 16, wherein within a time [said contents utilization control means is indicated to be according to said criteria from said reproduction start] regards it as said one use.

[Claim 18]A server apparatus which manages use of said contents via a transmission line to a terminal unit using contents which are digital works, comprising:

A right-information-data memory measure which memorizes right information data about a utilization right of contents which a user who uses said terminal unit owns.

A license ticket issuing means which generates a license ticket which is right information data which show a part of utilization right which the user concerned owns based on a demand from said user, and transmits to said terminal unit.

[Claim 19]The server apparatus according to claim 18, wherein said license ticket issuing means acquires a demand which specifies a part of utilization right which said user owns from the user concerned, generates a license ticket corresponding to the specification and transmits to said terminal unit.

[Claim 20]The server apparatus according to claim 18, wherein said license ticket issuing means generates a license ticket in which a utilization right of the minimum unit which constitutes a utilization right which said user owns is shown.

[Claim 21]Said server apparatus acquires further information about an external recording medium connected to the terminal unit concerned from said terminal unit based on a demand from said user, The server apparatus according to claim 18 provided with a judging means which judges whether it has a means by which said external recording medium controls use of said contents according to a utilization right which said license ticket shows.

[Claim 22]A terminal unit which obtains permission of a server apparatus via a transmission line, and uses contents which are digital works, comprising:

A reception means which receives a license ticket which is right information data which show a part of utilization right which a user owns from said server apparatus.

A contents utilization control means to control use of said contents according to a utilization right which a received license ticket shows.

[Claim 23]Said terminal unit is provided with a decoding means which decrypts further a license ticket received by said reception means, and said contents utilization control means, The terminal unit according to claim 22 characterized by controlling use of said contents according to a utilization right which a decrypted license ticket shows.

[Claim 24]The terminal unit according to claim 22 when it judges whether said license ticket permits use of further contents and does not approve [said contents utilization control means], after contents are used, wherein it cancels the license ticket concerned.

[Claim 25]Said terminal unit is provided with a still more nearly removable external recording medium, and said contents utilization control means, The terminal unit according to claim 24 characterized by storing the license ticket in said external recording medium when a license ticket in which after a license ticket before contents are used, and contents use permits use of further contents permits movement of contents.

[Claim 26]Said external recording medium connected to said terminal unit further said terminal unit, Have a judging means which judges whether it has a means to control use of said contents according to a utilization right which said license ticket shows, and said contents utilization control means, The terminal unit according to claim 25 characterized by storing a license ticket in an external recording medium when judged with said external recording medium being provided with said control means.

[Claim 27]The terminal unit according to claim 26 changing said contents utilization control means into contents control information on a format which is different in said license ticket when judged with said external recording medium not being provided with said control means.

[Claim 28]A contents use controlling method in a system which consists of a terminal unit using contents characterized by comprising the following which are digital works, and a server apparatus which manages use in said terminal unit of said contents via a transmission line.

A right-information-data memory step which memorizes right information data about

a utilization right of contents which a user for whom said server apparatus uses said terminal unit owns.

Based on a demand from said user, a license ticket which is right information data which show a part of utilization right which the user concerned owns is generated, A receiving step which receives a license ticket in which said terminal unit has been transmitted from said server apparatus including a license ticket issue step which transmits to said terminal unit.

A contents utilization control step which controls use of said contents according to a utilization right which a received license ticket shows.

[Claim 29]The contents use controlling method according to claim 28 acquiring a demand which specifies a part of utilization right which said user owns in said license ticket issue step from the user concerned, generating a license ticket corresponding to the specification, and transmitting to said terminal unit.

[Claim 30]A program as which a computer is operated as a means which is a program for a server apparatus in a contents use management system, and with which a server apparatus of a statement equips any 1 paragraph of claims 18–21, comprising:

A terminal unit using contents which are digital works.

A server apparatus which manages use in said terminal unit of said contents via a transmission line.

[Claim 31]A program as which a computer is operated as a means which is a program for a terminal unit in a contents use management system, and with which a terminal unit of a statement equips any 1 paragraph of claims 22–27, comprising:

A terminal unit using contents which are digital works.

A server apparatus which manages use in said terminal unit of said contents via a transmission line.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention enables it to carry out certainly and simply the right management and utilization control of the contents which restrict the reproduction frequency of contents, etc. especially about the system and method of managing the digital-contents use of music, an image, etc. distributed by communication, broadcast, etc.

[0002]

[Description of the Prior Art] In recent years, the system which distributes digital works, such as music, an image, a game, by the Internet, digital broadcasting, etc. is developed, and, as for the part, the stage of utilization is greeted. They are collectively examined by the right management of the contents which restrict the reproduction frequency of contents, movement, a duplicate which were distributed, and the method (DRM: Digital Rights Management) of utilization control from viewpoints of copyright protection etc. in distribution of these contents.

[0003] In the conventional digital-contents distribution system. The utilization condition over each user's contents is distributed to a receiver with contents, and the model is made so that all may be managed by the user terminal side, so that JP,2000-48076,A and JP,2000-293439,A may see.

[0004] For example, when a certain user purchases the right to which it views and listens 3 times about a movie "Matrix." A user terminal receives the utilization condition which shows that it is "possible [3 times viewing and listening of Matrix]" with the contents of a movie "Matrix" via communication from a distributing server, and manages reproduction of contents according to a utilization condition.

[0005] The distributing server does not participate in a user's utilization condition, after distributing the above-mentioned utilization condition to the user terminal. When reproducing the contents which the user terminal accumulated, and viewing and

listening to "Matrix", and processing which reduces the utilization condition which a user terminal manages every [1] is performed and the number of times to which it can be viewed and listened is set to 0 whenever it views and listens once, processing which makes viewing and listening disapproval is performed.

[0006]Drawing 17 shows the composition of the conventional digital-contents distribution system.

[0007]The user management data base 1001 which accumulates the ID information etc. of the user who did membership registration of the distributing server 1000, The contents information data base 1003 which accumulates the utilization condition of the contents key which enciphers contents, and contents, The contents database 1006 which accumulates contents, and the user authentication part 1002 which performs user authentication, The contents information generation part 1004 which generates contents information including the utilization condition of contents, and the information on a contents key, The contents information encryption section 1005 which enciphers contents information by the characteristic data of users, such as user ID, It has the contents acquisition section 1007 which acquires the contents specified from the contents database 1006, the contents encryption section 1008 which enciphers contents with a contents key, and the communications department 1009 with the user terminal 2000.

[0008]The communications department 2001 with which the user terminal 2000 communicates between the distributing servers 1000 on the other hand, The ID information accumulating part 2002 which accumulates ID information, and the accumulating part 2003 (HDD) which accumulates the enciphered contents, The contents information decoding part 2006 which decodes a contents key and a utilization condition from the received contents information, The utilization condition Management Department 2007 which manages the utilization condition and contents key of contents, The utilization condition treating part 2008 which processes the utilization condition at the time of contents playback, It has the contents decoding part 2005 which decodes contents with the contents key acquired from the utilization condition treating part 2008 when fulfilling a utilization condition, and the external media access part 2004 which outputs contents to the external media 5000.

[0009]Drawing 18 shows the process flow in case the user terminal 2000 purchases contents from the distributing server 1000 in this digital-contents distribution system.

[0010]If there is a user's content purchase demand, the communications department 2001 of the user terminal 2000 will acquire the ID information of the user terminal 2000 accumulated in the ID information accumulating part 2002, and will transmit this

ID information and a content purchase demand to the distributing server 1000 (S1001).

[0011]The user authentication part 1002 which received through the communications department 1009 of the distributing server 1000 this information, After comparing the received ID information with the ID information accumulated in the user management data base 1001 and performing user authentication, a content purchase demand is passed to the contents information generation part 1004 (S1002).

[0012]The contents information generation part 1004 performs accounting to content purchase, acquires the utilization condition of purchase contents, and the information on a contents key from the contents information data base 1003, and passes a contents key to the contents acquisition section 1007 with the information on purchase contents. Contents information including a utilization condition and the information on a contents key is generated, the contents information encryption section 1005 is passed, and the contents information encryption section 1005 enciphers contents information (S1003).

[0013]The contents acquisition section 1007 acquires contents applicable from the contents database 1006, and the contents encryption section 1008 enciphers these contents with a contents key (S1004).

[0014]The communications department 1009 of the distributing server 1000 transmits the enciphered contents and the enciphered contents information to the user terminal 2000.

[0015]The communications department 2001 of the user terminal 2000 receives the enciphered contents and the enciphered contents information including the information on a contents key and a utilization condition (S1005), sends contents to the accumulating part 2003, and accumulates them (S1006).

[0016]Contents information is sent to the contents information decoding part 2006. The contents information decoding part 2006 decrypts the contents information enciphered, takes out a utilization condition and a contents key, and accumulates them in the utilization condition Management Department 2007 (S1007).

[0017]Drawing 19 shows the process flow in case the user terminal 2000 reproduces contents in this digital-contents distribution system.

[0018]If there is a user's contents playback demand, the utilization condition treating part 2008 will acquire the applicable utilization condition and contents key of contents which are managed by the utilization condition Management Department 2007 (S2001), and will check the reproduction frequency (number of times which permits reproduction) of a utilization condition (S2002).

[0019]When reproduction frequency is larger than 0, the decrement of the

reproduction frequency of (S2003) and a utilization condition is carried out (S2004), and a utilization condition and a contents key are accumulated in the utilization condition Management Department 2007 (S2005).

[0020]The contents decoding part 2005 acquires contents applicable from the accumulating part 2003 (S2006), decodes contents using the contents key passed from the utilization condition treating part 2008, and reproduces contents (S2007). In Step S2003, when reproduction frequency is not larger than 0, regeneration is ended.

[0021]The image/sound of the reproduced contents are outputted to the monitor of TV etc. from the contents decoding part 2005. When moving to the external media 5000 or reproducing contents, the image/sound of contents are outputted to the external media 5000 via the external media access part 2004.

[0022]In order to prevent disclosure of confidential information, the ID information accumulating part 2002, the contents information decoding part 2006, and the utilization condition Management Department 2007 treating confidential information are usually established in security modules, such as an IC card, and the user terminal 2000 is equipped with this security module.

[0023]In this case, when sending the information on a utilization condition or a contents key to the utilization condition treating part 2008 from the utilization condition Management Department 2007, it is enciphered, these information is outputted from a security module, and the utilization condition treating part 2008 decrypts and uses these information. Also when accumulating the utilization condition which the utilization condition treating part 2008 updated in the utilization condition Management Department 2007, it is re-enciphered and is sent out to a security module.

[0024]In the conventional digital-contents distribution system, the utilization condition over each user's contents is managed by such a method at the user terminal side.

[0025]

[Problem(s) to be Solved by the Invention]However, in managing each user's utilization condition with a user terminal, there are the following problems.

(1) Complicated utilization condition management with a user terminal is required, and the function of a user terminal may be enlarged.

(2) Since a distributing server does not have a concern in use and right management processing of the distributed contents at all, even when the copy of contents, etc. are performed by the user terminal, it cannot pursue contents and cannot detect to what kind of medium it was copied when.

(3) When the accumulation means (HDD) of a user terminal crashes, restoration of a user's utilization condition etc. is difficult (in order for there to be nothing that holds the information except a user terminal).

(4) When carrying out service which is referred to as making automatic reproduction frequency of the utilization condition of purchased contents +1 if new contents are purchased or performing the addition of a new utilization condition, etc., a hard and soft change of both a distributing server and a user terminal is needed. Therefore, processing of the service which extends such a utilization condition, an addition of a utilization condition, etc. is difficult in practice.

[0026]All each user's utilization conditions are managed by the distributing server side, and a user terminal does not control a utilization condition, but they are the contents (.) themselves at a communication course at every viewing and listening. Or when contents are enciphered, the model in which only a contents key acquires C from a distributing server is also considered, but there are the following problems in this case. (5) Since utilization control to these contents is not performed after passing contents to a user terminal, in a user terminal, it becomes possible to use the acquired contents indefinitely (it reproduces especially).

[0027]This invention solves such a conventional problem and an object of this invention is for a server to provide the contents use management system which controls use of the contents in a user terminal certainly and simply, a contents use controlling method, etc., without hanging a burden on a user terminal.

[0028]

[Means for Solving the Problem]To achieve the above objects, a contents use management system concerning this invention, It is a contents use management system which consists of a terminal unit using contents which are digital works, and a server apparatus which manages use in said terminal unit of said contents via a transmission line, A right-information-data memory measure which memorizes right information data about a utilization right of contents which a user for whom said server apparatus uses said terminal unit owns, Based on a demand from said user, a license ticket which is right information data which show a part of utilization right which the user concerned owns is generated, Have a license ticket issuing means which transmits to said terminal unit, and said terminal unit, According to a reception means which receives a license ticket transmitted from said server apparatus, and a utilization right which a received license ticket shows, it has a contents utilization control means to control use of said contents.

[0029]In this specification, "use" of contents, "Reproduction", "movement" and a

“duplicate” of contents, “printing” of contents of a digital book, etc. include all the operations which use contents, and further as anticipation of these operations, Downloading “license information” (download a license ticket beforehand) shall also contain.

[0030]Here said license ticket issuing means, A demand which specifies a part of utilization right which said user owns is acquired from the user concerned, A license ticket corresponding to the specification is generable, it can transmit to said terminal unit, or a license ticket in which a utilization right of the minimum unit which constitutes a utilization right which said user owns is shown can be generated, and it can also be characterized by transmitting to said terminal unit. According to this composition, a using state of contents in each terminal unit can be grasped finely, or management load of a utilization right in each terminal unit can be made into the minimum.

[0031]It can also be made said license ticket whether the contents of the license ticket concerned were altered with composition in which detection information for detecting is included. Thereby, an alteration of a license ticket can be prevented certainly.

[0032]Realize this invention as a server apparatus and a terminal unit which constitute the above-mentioned contents use management system, or, It can realize as a contents use controlling method which uses as a step a characteristic means to constitute these server apparatus and a terminal unit, or can also realize as a program which makes a personal computer etc. perform these steps. And it cannot be overemphasized that the program can be widely circulated via transmission media, such as recording media, such as DVD, and the Internet.

[0033]

[Embodiment of the Invention]Hereafter, an embodiment of the invention is described in detail using a drawing. Drawing 1 is a figure showing the composition of the whole contents use management system 1 concerning this embodiment.

[0034]The center side serves as a subject and this contents use management system 1 manages dynamically the use right (license) for every contents given to the user who purchased digitized contents, such as music, a movie, books, By enabling it to use contents within the limits of the utilization condition which distributes the license ticket (it is hereafter described also as “LT”.) for using contents based on a user’s demand, and is included in LT. It is a system which protects the copyright of contents and comprises the server 100 allocated by the center, the user terminals 200a–200c which the user using contents uses, and the communication network 300 which

connects these.

[0035]The servers 100 are computers, such as a workstation, and function as a user managing server, a contents distribution server, a fee collection server, and a license management server. The server 100 manages the user who joined this system 1, and the terminal which the user owns, or specifically. Receive the purchase of contents from the user terminals 200a-200c etc., or, The license ticket issue requesting from the user terminals 200a-200c etc. (it is hereafter described also as "LT issue requesting".) -- the Web page to receive, [have and] Charge according to the content purchase demand from the user terminals 200a-200c, and the enciphered contents are distributed to the user terminals 200a-200c, or LT for using the contents enciphered according to LT issue requesting with the user terminals 200a-200c is distributed. This LT is provided with the following.

The contents key for decrypting the enciphered contents.

The logging utilization condition which started the part out of the use right (license) given to the user about contents.

[0036]The user terminals 200a-200c are computer paraphernalia, such as a personal computer, a Personal Digital Assistant, and a digital television, and function as a client to the server 100. Specifically the user terminals 200a-200c, According to a user's operation, the Web page of the server 100 is accessed using tools, such as the Internet browser software, A content purchase demand is transmitted, distribution of contents is received, or LT issue requesting is transmitted in use of contents, LT is received, and contents are reproduced in the range of the logging utilization condition of LT.

[0037]To the user terminal 200a, the external media 500b for the user terminals 200b. (For example, SD card) The external media 500c for the user terminals 200c. It can equip with (for example, an IC card), contents and LT which the user terminal 200a holds are copied to the external media 500b and 500c, or it moves, and it is constituted so that contents can be reproduced with the user terminals 200b and 200c.

[0038]The communication networks 300 are the communication media by cables, such as the Internet and CATV, and radio, such as digital broadcasting.

[0039]Drawing 2 is a functional block diagram showing the composition of the server 100 and the user terminals 200a-200c which are shown in drawing 1. Since it is the same about the functional constitution of the user terminals 200a-200c, the user terminal 200a is illustrated as the representative. The communication network 300 is

also collectively shown in this figure.

[0040]The data division (user management DB110, user right-information-data DB120, contents information DB130, contents DB140) realized with the data file etc. which roughly divided the server 100 and were stored in the hard disk etc., CPU, RAM, By the program etc. which are executed by hardware and CPUs, such as ROM. It consists of a treating part (the user authentication part 150, the user right processing part 160, the license information generation part 165, the contents information generation part 170, the contents information encryption section 175, the contents acquisition section 180, the contents encryption section 185, the communications department 190) realized.

[0041]User management DB110 accumulates a user's User Information etc. which carried out membership registration to this contents use management system 1. In order that user management DB110 may manage a user's right, specifically, Client ID of the user terminal which the user who matches with User Information containing user ID, manages using unique client ID (terminal ID) assigned for every user terminal, and did membership registration owns, It is a storage parts store which memorizes two or more user management tables 111 for registering and managing the peculiar ID information (user ID) given to the user, the user's User Information, etc.

[0042]User right-information-data DB120 accumulates a user's right information data (license) over contents. The contents to which the user specifically purchased user right-information-data DB120, It is a storage parts store which memorizes two or more user right-information-data management tables 121 for managing the residual information on the right of use (license) which a user has to the contents in every [of use] modes (for example, reproduction, movement, a copy, printing, an available term, etc.).

[0043]Contents information DB130 accumulates the pertinent information on contents (contents key etc.). Specifically, contents information DB130 holds the contents key table 132 grade which recorded the correspondence relation of two or more contents keys 131, and the contents key 131 and content ID for enciphering contents.

[0044]Contents DB140 accumulates contents. Specifically, contents DB140 accumulates and holds the content table 142 which recorded the correspondence relation between two or more contents 141, and its contents and content ID.

[0045]The user authentication part 150 performs user authentication. Specifically, the user authentication part 150 specifies user ID and the right managed by a server using the user management table 111 from the ID information (client ID) included in the

content purchase demand received from the user terminals 200a-200c, or LT issue requesting. The user authentication part 150 updates User Information of the user management table 111, when a user's address etc. are changed, or when a user's terminal unit is purchased, it adds client ID to the user management table 111.

[0046]The user right processing part 160 registers a user's right information data over contents according to a purchase request, or updates right information data according to a utilization request. Specifically, the user right processing part 160 registers the user's right into the user right-information-data management table 121 of user right-information-data DB120, after performing accounting according to a content purchase demand.

[0047]Since the accounting itself is not the essence of this invention, the portion which performs accounting has not been indicated to a figure. In the case of registration of a user's right, the initial value which the contents provider set up as UR-Us (Usage Rule for User on server) which is a user's right information data managed by a server is given. It is checked whether if the user right processing part 160 has LT issue requesting, it can start to a user right-of-use UR-Uc (Usage Rule for User on client) to have been required from right-information-data UR-Us at the time, Right-of-use UR-Uc required as being checked is passed to the license information generation part 165, and it updates by the contents which started right-information-data UR-Us managed by a server, and carried out the decrement only of part UR-Uc. The user right processing part 160 updates each contents purchaser's license information uniformly, when there is a notice which increases using frequency by the notice of change of right information data, for example, the service to a contents purchaser, from a contents provider, or extends an available term.

[0048]The license information generation part 165 generates the right of use of the requested contents, and license information.

[0049]The contents information generation part 170 acquires a contents key from contents information DB130, or generates contents information (LT) including the license information passed from the license information generation part 165, and the acquired information on a contents key. Specifically the contents information generation part 170, Access contents information DB130, and acquire the contents key 131 corresponding to content ID using the contents key table 132, or, LT including this contents key, and the license information passed from the license information generation part 165 and a logging utilization condition (UR-Uc) is generated.

[0050]The contents information encryption section 175 enciphers contents

information. Specifically, the contents information encryption section 175 enciphers this footer if needed, when the contents key of LT and the footer are added. This encryption is enciphered by terminal ID (client ID) of the user terminals 200a-200c which emitted LT issue requesting, for example. Thus, LT can be bound to the user terminal which has the client ID if it enciphers by client ID.

[0051]It may encipher by a user's public key using a public-key crypto system. It may encipher using the secret key shared between the server and the terminal.

[0052]SAC (Secure Authenticated Channel: with attestation safe channel) is formed between the server 100, the user terminal 200a - 200c, for example in the mutual recognition form by SSL (Secure Sockets Layer) etc., When a secure channel is secured between a server and a terminal, encryption of license information is arbitrary (it is not indispensable). However, by this embodiment, SAC is formed between server terminals and it explains as what performs encryption processing of LT by the contents information encryption section 175.

[0053]The contents acquisition section 180 acquires the specified contents from contents DB140. With reference to the content table 142 of contents DB140, the contents acquisition section 180 acquires the contents 141 corresponding to content ID, and, specifically, passes them to the contents encryption section 185.

[0054]The contents encryption section 185 enciphers contents. Specifically, the contents encryption section 185 enciphers the contents passed from the contents encryption section 185. This encryption is enciphered with a contents key.

[0055]The communications department 190 communicates with the user terminal 200. The communications department 190 is specifically a communication interface realized by the script described by the Web page which communicates with the user terminals 200a-200c via the communication network 300, a program, etc., Analyze the command and message which have been transmitted from the user terminals 200a-200c, or, According to the result, request processing from the user authentication part 150, distribute the contents passed from the contents encryption section 185 to the user terminals 200a-200c, or, LT passed from the contents information encryption section 175 is distributed to the user terminals 200a-200c, or SAC is formed between terminals.

[0056]On the other hand, the user terminal 200 is provided with the following.

Communications department 210.

Final controlling element 220.

ID information accumulating part 230.

The contents accumulating part 240, the LT accumulating part 245, the contents

information decoding part 250, the license information treating part 260, the contents decoding part 270, and the external media access part 280.

[0057]The communications department 210 communicates between the servers 100. The communications department 210 is specifically a communication interface which communicates with the server 100 via the communication network 300 according to browser software etc., According to the request from the final controlling element 220, transmit the message of a content purchase demand and LT issue requesting, or, Store in the contents accumulating part 240 the contents transmitted from the server 100, LT is stored in the LT accumulating part 245, or SAC is formed among the communications departments 190 of the server 100.

[0058]The final controlling element 220 is a user interface which receives a user's operation or displays the Web page which the server 100 provides.

[0059]The ID information accumulating part 230 accumulates the ID information (client ID) of the terminal. Specifically, the ID information accumulating part 230 carries out accumulation maintenance of peculiar client ID beforehand embedded for every terminal. The ID information accumulating part 230 may hold the public key of the public-key crypto system for enciphering LT, a secret key, or the encryption key of a common key encryption system.

[0060]The contents accumulating part 240 comprises HDD etc. and accumulates the enciphered contents, for example. The LT accumulating part 245 accumulates LT sent from the communications department 210.

[0061]The contents information decoding part 250 decodes a contents key and license information from the received contents information (LT). Specifically, the contents information decoding part 250 decrypts the contents key etc. which are contained in LT accumulated in the LT accumulating part 245 with client ID, the secret key of a public-key crypto system, or the secret key of a common cipher system.

[0062]The license information treating part 260 identifies the propriety of use of a contents key based on license information. It judges whether the license information treating part 260 is refreshable, if refreshable, a contents key will be passed to the contents decoding part 270, and specifically, it supervises so that it may start in the contents playback processing by the contents decoding part 270 and a utilization condition may be kept.

[0063]The contents decoding part 270 decrypts the contents enciphered with the contents key acquired from the license information treating part 260. The contents

decoding part 270 decrypts the enciphered contents with the contents key got from the license information treating part 260, and, specifically, reproduces contents under management by the license information treating part 260.

[0064]The external media access part 280 outputs contents and either of the LTs, or both to the external media 500b or the external media 500c.

[0065]The above-mentioned ID information accumulating part 230, the LT accumulating part 245, the contents information decoding part 250, and the license information treating part 260 are formed in the secure module Tampa[-proof]-ized in hardware, for example, the IC card in which the chip was built. In this case, a security module may perform decoding of license information and the processing of license information which were enciphered. However, where SAC is established, when LT is acquired from a server, since encryption of license information is arbitrary, only when license information is enciphered, it performs decoding processing. For this reason, it makes it impossible to access from the outside important confidential information, the contents key contained in the clients ID and LT, a utilization condition, etc. on copyright protection, and has become a strong design also to the hard attack which tries to steal such confidential information physically. Here, the Tampa[-proof]-ized software may be sufficient as a security module. The license information treating part 260 may be formed in the secure portion of a user terminal.

[0066]In the contents use management system 1 constituted in this way, the right information data over each user's contents are fundamentally managed altogether by the distributing server side. The contents which the user purchased (or prior contract) are accumulated in the contents accumulating part 240 of the user terminal 200a in the state where it was enciphered. When reproducing the contents accumulated in the user terminal 200 or performing movement and reproduction, a request and LT issue requesting message are sent from the user terminal 200 to the server 100. The server 100 distributes the contents information and LT which contain "license information" and a contents key to a user, when utilization condition (or conditions of contract) UR-Us to the contents which the user requested is checked and a user's right of use exists. License information comprises propriety information, including reproduction of contents, movement, a duplicate, etc., and a user terminal performs use of the contents permitted by license information.

[0067]When a user acquires each contents by purchase etc., the utilization condition about the contents which the user acquired is managed by user right-information-data DB120 of the server 100. this form -- each time -- a purchased type -- it is called a model. In addition to this, this system can also apply

the model of a subscribed mold (prior contract type). It is a fee collection gestalt which is referred to as this subscribed mold being a thing of a gestalt like the Tia fee collection as used in the field of broadcast, and being able to watch all the programs of an applicable channel if a channel contract is performed. In this case, contract information is held as user right information data user right-information-data DB120. [0068]Drawing 3 is a figure showing the example of composition of the user management table 111 shown in drawing 2.

[0069]The user ID given to the user by whom this user management table 111 joined this contents use management system 1, User Information (a "name" and an "address".) related with this user ID "The telephone number 1", the "telephone number 2", --, "E-mail1", "E-mail2", It is constituted by --), client ID ("client ID1", "client ID2", "client ID3", --) beforehand given to the user terminal which this user uses with this contents use management system 1, etc. According to the user management table 111 constituted in this way, if client ID is known, the user ID of the user who owns the terminal equipment of the client ID can be specified.

[0070]Drawing 4 is a figure showing the example of composition of the user right-information-data management table 121 shown in drawing 2.

[0071]This user right-information-data management table 121 Client ID or user ID, It is constituted by the residual information etc. which are set to the content ID of the contents which the user purchased, and ID of the right of use (UR-Us) of the user who is set up for every content ID and manages by a server for every mode of use of the right of use (license) which a user has. Or [that the residual information set up for every mode of use can reproduce the contents which each user purchased how many times in the back], It is shown, respectively how many times the back can move the contents how many times, or the back can copy the contents, till when the contents can be used, or how many copies of the contents the back can print. The longest utilization time set as residual information by being attached shows the maximum time which can use contents continuously in regeneration etc., time for a judgment threshold to judge use of contents to be 1 time once is shown, and the accumulation utilization time shows the accumulated time which can use contents.

[0072]According to the attribute of contents, the initial value is beforehand defined for the contents provider or the administrator of the server for every contents, and, as for the contents of the right of use, an initial value is given as residual information on a license at the time of content purchase. If the same contents are also in the sales styles that a price changes with utilization conditions which a user can acquire here, it may be an initial value which changes with purchase price. And the decrement

of the residual information on this license is carried out one by one from every [a utilization condition, / license information], and the initial value which are started according to a user's LT issue requesting, or it *****s it according to a contents provider's service provision request.

[0073]In this user right-information-data management table 121, although the right of use was managed by user ID, a user's right of use may be managed using client ID.

[0074]Drawing 5 is a figure showing the example of composition of the license information shown in drawing 2.

[0075]This license information is generated for the information on the started right of use, for example, the minimum utilization condition element of a utilization condition, 1 or two or more propriety information about use of contents are comprised, and each propriety information comprises a parameter only showing propriety. Here, alpha shown in drawing 5 is the propriety information about action and reproduction, the propriety information concerning [beta shown in drawing 5] action and movement, and the propriety information concerning [gamma shown in drawing 5] action and a duplicate. The kind and number of these propriety information change with the attributes of contents.

[0076]Here, although the case of the minimum right of use was explained, when a user requires, license information including the utilization condition of not only the demanded part logging right of use, i.e., propriety, but the multiple times in the case of being good may be generated. Although one license information shows the example which comprises conditions about two or more contents use by drawing 5, it is also possible to constitute license information as respectively independent information, to summarize two or more them, and to treat as license information over one contents.

[0077]Drawing 6 is the contents information generated by the contents information generation part 170 and a figure showing the data format composition of LT.

[0078]LT600 generated by the contents information generation part 170, The LT header 610 and action which is license information, i.e., the contents of operation of contents, It comprises 1 or two or more LT action tag blocks 620#1 – 620#n showing the conditions over action, etc., the LT contents key tag block 630, and the LT footer 640.

[0079]The LT identifier 611 showing the LT header 610 being a license ticket with which this data is treated with this contents use management system 1, The version number 612 which shows the version of the specification defined with this contents use management system 1, The LT size 613 which shows the data size of the whole LT, and the content ID 614 which shows the content ID of the contents with which

this LT is related, UR-Us ID615 which shows ID of UR-Us which became the issue origin of this LT, The start time 616 of LT term of validity which shows the time to which this LT becomes effective, LT move permit flag 618 which shows whether the finish time 617 of LT term of validity which shows the time to which LT becomes invalid, the contents from a certain user terminal to portability external media or another user terminal or movement of LT, etc. is permitted, It comprises the LT encryption method 619 which shows LT contents key tag block 630 and the cipher systems (DES, AES, etc.) applied to the LT footer 640.

[0080]LT action tag block 620#1 – 620#n, Action ID621 which shows ID which specifies the contents of action over contents, The longest utilization time 622 which shows the maximum time which can operate contents continuously, It comprises the 1-time judging threshold 623 which shows time to judge operation of contents to be 1 time, the frequency counter 624 in which the maximum times which can operate contents by this LT are shown, and the accumulation utilization time 625 which shows the operate time of the accumulation which can operate contents. Even when contents interrupt reproduction temporarily for a toilet, for example in the case of the movie of 2 hours, etc. (pause), the longest utilization time is set as a value (for example, 4 hours) usually longer than 2 hours so that he can see a movie to the last. The accumulation utilization time is used when performing utilization control stricter than the longest utilization time, and it is usually set as a value (for example, 3 hours) shorter than the longest utilization time longer than 2 hours.

[0081]Here, when the 1-time judging threshold 623 is "0" and contents operation (use) is started in the user terminal 200a, it is judged with 1 time, and when specification is carried out, if a certain time reaches at the time, it will be judged to be 1 time. Whenever the value set as the frequency counter 624 operates contents, it is subtracted. However, it is subtracted when a 1-time judging threshold is effective, and the continuous operation time of contents reaches the value of a judgment threshold once (when there is nothing "0"). While carrying out continuous operation, subtraction of a frequency counter is performed only once. The time set as the longest utilization time 622 and the accumulation utilization time 625 is subtracted according to the operate time of contents. However, in a pause, subtraction is stopped at the time when the time set as the longest utilization time 622 was set as the accumulation utilization time 625 although the inside of a pause was also subtracted. If the value of the frequency counter 624 is one or more and it is 0 about C, a failure is expressed, and if it is 1, the minimum utilization condition is expressed. Therefore, the frequency counter 624 can also be used as propriety information.

[0082]The decode key and contents key which solve the code of contents in which LT contents key tag block 630 was related with this LT are stored.

[0083]When it is [whether the LT footer 640 adds and] the block of arbitrary options and is added, In order to prevent the alteration of the portion from the LT header 610 to just before [630] the LT footer 640 (i.e., LT contents key tag block), the hash value by SHA-1 algorithm is stored.

[0084]Although content ID was stored in the LT header 610 in this LT600, It is set up as an identifier for content ID to associate contents information and contents, and since it is an important thing whose specification of contents information is attained from the content ID acquired to contents utilization time by this, it may store in a tag block.

[0085>About the contents use management system 1 in the embodiment of the invention constituted as mentioned above, the operation at the time of content purchase is explained using the flow chart shown in drawing 7 below.

[0086]Drawing 7 is a flow chart which shows the processing performed, respectively by the user terminal 200a and the server 100 in case a user purchases contents in this system.

[0087]When purchasing contents, the user of the user terminal 200a operates the final controlling element 220, accesses the Web page of the server 100, and calls the content purchase screen (1) shown in drawing 8.

[0088]This content purchase screen (1) The display of the genre of the contents in which net purchase by this system is possible, "music", a "game", a "digital book", a "movie", --, a "pay-television program", It comprises a check box which chooses these genres, a "next" button, the button "returning", etc.

[0089]When the genre of contents to purchase is music, a user operates the final controlling element 220, clicks the check box corresponding to "music", and does the depression of the "next" button. The content purchase screen (2) shown in drawing 9 by this is displayed.

[0090]This content purchase screen (2) comprises contents of "content ID" of the music belonging to a genre and music, a "title name", "right information data", and the "selling price", a check box which chooses these music, "purchase" button, the button "returning", etc. The initial value of the utilization condition which the contents provider set up of being main, i.e., residual information, reproduction frequency, the number of times of movement, the number of times of a copy, an available term, etc. are shown in "right information data." When music to purchase is "surfing George", a user operates the final controlling element 220, clicks the check box corresponding to

"surfing George", pushes "purchase" button, and inputs a content purchase demand. [0091]When there is a user's content purchase demand, the communications department 210 of the user terminal 200a, After forming SAC among the communications departments 190 of the server 100, the ID information (client ID) of the user terminal 200 accumulated in the ID information accumulating part 230 is acquired, and a content purchase request message including this ID information is transmitted to the server 100 (S1). This content purchase request message comprises content ID of the message ID showing content purchase, and the contents which wish to purchase, client ID of the user terminal which requires content purchase, etc., for example.

[0092]If this information is received through the communications department 190 of the server 100, after the user authentication part 150 will compare the received ID information with the ID information accumulated in user management DB110 and will perform user authentication, it passes a content purchase demand to the user right processing part 160 (S2). Specifically, the user authentication part 150 passes user ID, content ID, etc. to the user right processing part 160 as a content purchase demand, after specifying user ID from client ID with reference to the user management table 111.

[0093]The user right processing part 160 registers a user's right information data over purchase contents into user right-information-data DB120, after performing accounting of content purchase (S3). the user (for example, the east ****) who the user right processing part 160 accesses user right-information-data DB120, and specifically purchases contents -- the user right-information-data management table 121 (refer to drawing 4) of business is specified from user ID "pana01." And the user right processing part 160 stores the music 1 in the column of the content ID of the user right-information-data management table 121, respectively, and stores ID of right-information-data UR-Us of the music 1, the "right information data A", and its contents in the column of the license information for every content ID, respectively. The residual information on the initial value which the contents provider set up, including reproduction frequency, the number of times of movement, the number of times of a copy, etc., is set to the contents of these right information data A. And the user right processing part 160 passes content ID to the contents information generation part 170.

[0094]The contents information generation part 170 acquires the pertinent information on applicable contents (contents key etc.) from contents information DB130, and passes it to the contents acquisition section 180 (S4). The contents

information generation part 170 accesses contents information DB130, acquires the contents key 131 corresponding to content ID with reference to the contents key table 132, and, specifically, passes the contents key and content ID which were acquired to the contents acquisition section 180.

[0095]The contents acquisition section 180 acquires applicable contents from contents DB140, and the contents encryption section 185 enciphers these contents with a contents key (S5). The contents acquisition section 180 accesses contents DB140, and the contents corresponding to content ID are specifically acquired with reference to the content table 142, The acquired contents, the contents key received from the contents information generation part 170, and client ID are passed to the contents encryption section 185. The contents encryption section 185 enciphers the received contents with a contents key, and passes the communications department 190 the enciphered contents. The communications department 190 of the server 100 transmits the enciphered contents to the user terminal 200 (S5).

[0096]Contents will be sent to the contents accumulating part 240, and the communications department 210 of the user terminal 200 will accumulate them, if the enciphered contents are received (S6) (S7). By execution of each processing of such a user terminal 200a and the server 100, the session at the time of content purchase is completed.

[0097]In the session at the time of content purchase, since SAC is formed between the user terminal 200a-servers 100 and encryption communication is performed by the common session key, the decipherment on the network of a content purchase request message can be prevented.

[0098]Drawing 10 is a flow chart which shows the processing performed, respectively by the user terminal 200a and the server 100 in case a user uses contents in this system.

[0099]When using contents, the user of the user terminal 200a operates the final controlling element 220, and displays the use contents selection picture shown in drawing 11. The title of the contents to which the user of the user terminal 200a purchased this use contents selection picture, content ID, Or it comprises a prior application etc. of the license ticket about the contents a contract of was made in advance, a check box about these contents, a "next" button, a button "returning", etc.

[0100]When using contents, a user inputs the use information on the contents which operate the final controlling element 220 and are reproduced. A user displays the use contents selection picture shown in drawing 11, inputs a check mark into the check

box of the contents (for example, surfing George) which wish to reproduce, and, specifically, clicks a "next" button. And the contents utilization request screen shown in drawing 12 is displayed. A contents utilization request screen is constituted from available action, reproduction, movement, a copy, the check box which chooses this action, the text box which inputs the number of times of action and "determination" button, the button "returning", etc. by these contents.

[0101]A user operates the final controlling element 220 as part of the input of use information, A request content required about selected contents (surfing George) (in this example) [and] The number of demands (this example reproduction "2" times and movement "1" time) is inputted into the text box of a request content which put the check mark into the check box of movement and into which the check mark was put, and "determination" button is clicked.

[0102]If a check mark is put into a check box, "1" will be beforehand inputted into the text box as a utilization condition of *****. And what is necessary is just to input the number of times to want into a text box, when a user wants the use more than "2" times.

[0103]When there is a user's contents playback demand, the communications department 210 of the user terminal 200, After forming the communications department 190 and SAC of the server 100, the ID information (client ID) of the user terminal 200 accumulated in the ID information accumulating part 230 is acquired, and LT issue requesting message including this ID information is transmitted to the server 100 (S11). The content ID (for example, music 1) of the contents the message ID to which this LT issue requesting message expresses LT issue requesting, for example, and for use, It comprises client ID (for example, nat01) etc. of the user terminal which requires LT issue as the demand information (two reproduction, one movement) showing the contents of a contents playback demand, i.e., a contents utilization request.

[0104]After the user authentication part 150 which received this information through the communications department 190 of the server 100 compares the received ID information with the ID information accumulated in user management DB110 and performs user authentication, it passes User Information and a contents playback demand to the user right processing part 160 (S12). Specifically, the user authentication part 150 passes client ID, content ID, demand information, etc. to the user right processing part 160 as a contents playback demand with user ID, after specifying user ID from client ID with reference to the user management table 111.

[0105]The user right processing part 160 checks a user's right information data over

the requested contents registered into user right-information-data DB120 (S13). the user (for example, the east ****) who the user right processing part 160 accesses user right-information-data DB120, and specifically uses contents -- the user right-information-data management table 121 (refer to drawing 4) of business is specified from user ID "pana01." And the user right processing part 160 checks whether reproduction and movement are included in the residual information (UR-Us) on the music 1, or the number of times required of reproduction and movement remains with reference to the column of the content ID of the user right-information-data management table 121, and the music 1.

[0106]The check of the right information data of the user in the case of a subscribed mold (prior contract type), It is carried out by attaching and judging, without whether containing contents with a request in which subscription (contract), and the user having the subscription concerned.

[0107]When the right information data of the reproduction to the contents requested into the registered right information data are included, (S14) and the user right processing part 160, Reproductive propriety is told to the license information generation part 165 based on the right information data, the contents of reproductive right information data are updated (decrement of the number of times of refreshable), and it stores in user right-information-data DB120 (S15). The license information generation part 165 generates license information based on the information given from the user right processing part 160, and passes it to the contents information generation part 170 (S15). As shown in drawing 13, specifically the user right processing part 160, The residual information on the content ID of user ID "pana01", reproduction frequency "10 times", "Twice" the number of times of movement, and the number of times of a copy "3 times" "8 times", reproduction frequency, the number of times of movement "1 time", From 3 times, update to the number of times of a copy "3 times", namely, about reproduction, decrease from 10 times to 8 times, decrease 2 times about movement, and a utilization condition (UR-Us) the license information generation part 165, The license information of "2 times", reproduction frequency, and the number of times of movement "1 time" is passed to the contents information generation part 170, and it is made to send to the user terminal 200a as an LT.

[0108]The use right which does not fill the use right demanded from the user terminal by judgment by the side of a server can also be transmitted as an LT. For example, even when a reproductive right is required twice from a user terminal, it becomes possible to secure the policy of transmitting the minimum use right each time, by

business judgment etc. by transmitting 1 time of a reproduction right as an LT.

[0109]The contents information generation part 170 reads the information on the contents key of applicable contents from contents information DB130, and generates contents information (LT) including this contents key and license information (S16). Specifically the contents information generation part 170, By the LT header 610, and action and reproduction, by LT action tag block 620#1 of the value "2" of a frequency counter, and action and movement. LT600 which consists of LT action tag block 620#2 of the value "1" of a frequency counter, the LT contents key tag block 630, and the LT footer 640 is generated. The contents information encryption section 175 enciphers this contents information (S16). Specifically, the contents information encryption section 175 enciphers LT contents key tag block 630 and the LT footer 640.

[0110]The communications department 190 of the server 100 transmits to the user terminal 200 by setting to LT the contents key and license information which were enciphered.

[0111]In Step S14, when the right information data of the reproduction about the contents requested into a user's right information data are not included, a reproduction improper response message is transmitted to the user terminal 200 from the server 100. The message ID which expresses that it is a response to LT issue requesting message, for example, and UR-Us applicable to a demand do not exist, but this reproduction improper response message comprises status ID showing being unreproducible.

[0112]On the other hand, in the user terminal 200, the communications department 210 which received contents information sends LT and client ID stored in the ID information accumulating part 230 to the contents information decoding part 250, after storing LT in the LT accumulating part 245 (S18). The contents information decoding part 250 decrypts the enciphered contents information (LT) by client ID, and passes license information and a contents key to the license information treating part 260 (S18).

[0113]The license information treating part 260 checks the reproduction propriety information on license information (S19), and when reproduction is good, it passes a contents key to (S20) and the contents decoding part 270. The license information treating part 260 confirms whether the frequency counter of action and reproduction is one or more, and when it is one or more, specifically, it passes a contents key to the contents decoding part 270. The contents decoding part 270 acquires contents from the contents accumulating part 240 (S21), contents are decoded with a contents key

and the music 1 "surfing George" is reproduced under management by the logging utilization condition of the license information treating part 260 (S22).

[0114]By the way, a judgment threshold, the longest utilization time, and the accumulation utilization time are included in LT action tag block 620#1 of action and reproduction once besides the value of a frequency counter.

[0115]For this reason, fixed time can be changed by taking the method judged to be that to which one reproduction was performed, when fixed time has passed since the reproduction start, and distributing the information on this fixed time from a distributing server about reproduction of the contents in a user terminal.

[0116]If it is in [from a reproduction start] fixed time as what it is at the reproduction start time and was reproduced once, it is regarded as the same reproduction, and it is also possible to take the method referred to as to permit reproduction, it can distribute the information which shows this range, and can also make it a reproductive time limit once.

[0117]That is, as shown in drawing 14, there is nothing that have been made once into the judgment threshold and for which the reproduction will be counted among 1 time in reproduction (for example, pre reproduction of search etc., etc.) of less than the time if time setting is carried out. And a judgment threshold can be reached once and it can be made to count among one reproduction for the first time. If time to be in the longest utilization time is set up, since the contents can be reproduced intermittently, the flexible usage pattern that a halt (pause) is possible during reproduction is realizable only by consuming 1 time of a reproduction right, until it reaches the longest utilization time. If time to be in the accumulation utilization time is set up, accumulation reproduction of the contents can be carried out until it reaches the accumulation utilization time. Therefore, various contents use can be provided to a user.

[0118]It may be made to change the policy about the judging method of such a refreshable period according to contents classification (for example, a movie and music).

[0119]When a reproduction improper response message is received from the server 100 (S17), when license information cannot be reproduced, processing is ended in Step S20, without reproducing contents. Here, a notice of being unreproducible is performed by the response message formed by existing [right-of-use UR-Us applicable to a demand]-for example, **** status code ERROR_URUS. A reproduction failure may be notified by LT including LT action tag block 620 which set the value of the reproduction frequency counter to "0."

[0120]When license information has specified only one use of contents, after the license information treating part 260 uses contents, it sets up the flag etc. which delete this license information or show an invalid thing, and performs processing which cancels license information (LT).

[0121]When license information treats them as license information over one contents collectively including the conditions (for example, reproduction and movement) of two or more actions, only the used conditions (for example, reproduction) concerned are cancelled.

[0122]Also with a subscribed mold, if unrestricted use may be accepted (for example, Tia fee collection), the maximum of a utilization condition may be provided in each contents (for example, being PPV (Pay Per View) monthly amount maximum of 5000 yen, etc.). When there is a maximum of a utilization condition, after judging said contract in the case of the check of a user's right information data, it will be judged whether the user has a utilization condition of the contents concerned (each time judgment of a contract type). It separates into the database of contract information, and the database of a utilization condition, and may be made to manage user right-information-data DB120.

[0123]Here in this contents use management system 1. It is possible to move right information data (utilization condition) and a contents key to the external media 500b and 500c with contents via the external media access part 280 by license information, when movement and the duplicate of contents are "practicable". At this time, after changing right information data into the data format currently supported by the external media 500b and 500c, they perform movement and reproduction. It is changed into the encryption key corresponding to the cipher system with which cipher converting (re-encryption) is carried out with the cipher system currently supported by the external media 500b and 500c, and the contents key is similarly supported by the external media 500b and 500c also about contents. Thus, use of contents is attained, planning copyright protection of contents by using external media with contents management method with this another contents use management system 1. However, when external media can support the contents use management system 1 of this invention, the data conversion of right information data and the cipher converting of contents are unnecessary.

[0124]Drawing 15 is a flow chart which shows the processing performed with the user terminal 200a in the case of moving contents or LT to external media in this system.

[0125]When moving contents or LT, the user of the user terminal 200a operates the final controlling element 220, and displays the move contents selection picture shown

in drawing 16. This move contents selection picture comprises a title of the contents which the user of the user terminal 200a purchased, content ID or a license ticket received beforehand, these contents, the check box about LT, "determination" button, etc. A user displays the use contents selection picture shown in drawing 16, inputs a check mark into the check box of the contents (for example, surfing George) which wish to move, and clicks "determination" button.

[0126]If there is a user's contents move demand, the license information treating part 260 of the user terminal 200a will pass client ID stored in the ID information accumulating part 230, and LT accumulated in the LT accumulating part 245 to the contents information decoding part 250. The contents information decoding part 250 decrypts the enciphered contents information (LT) by client ID, and passes license information and a contents key to the license information treating part 260.

[0127]The license information treating part 260 checks the move propriety information on license information, It is judged whether the value of the frequency counter of LT action tag block 620#2 of whether use is good and action, i.e., movement, is one or more (when it is ["possible / use after use /"] "before use") (S31). If use is good (it is Yes at S31), it will be judged whether the external media 500b or the external media 500c can process LT via the contents decoding part 270 and the external media access part 280 (S32).

[0128]If processing is not possible (it is No at S32), it will be judged whether the license information treating part 260 carries out format conversion of the utilization condition to the information changed into contents control information (S33). That is, the license information treating part 260 judges whether the external media 500b or the external media 500c can manage by the secure module Tampa[-proof]-ized in contents by contents control information. If manageable, the license information treating part 260 will change LT action tag block 620#2 of movement into contents control information (S34), and will pass the contents control information and the contents key which were changed to the contents decoding part 270. The contents decoding part 270 acquires contents from the contents accumulating part 240, decodes contents with a contents key and passes the decrypted contents and the contents control information passed from the license information treating part 260 to the external media access part 280. The external media access part 280 moves the decryption contents and contents control information which were passed from the contents decoding part 270 to the external media 500b or the external media 500c (S35).

[0129]If processing is possible in Step S32, the license information treating part 260

will pass LT to the contents decoding part 270. The contents decoding part 270 acquires contents from the contents accumulating part 240, decodes contents with a contents key and passes the decrypted contents and LT passed from the license information treating part 260 to the external media access part 280. The external media access part 280 moves the decryption contents and LT which were passed from the contents decoding part 270 to the external media 500b or the external media 500c (S35). In this case, the contents decoding part 270 is passed to the external media access part 280, without decrypting contents, and the external media access part 280 may move to the external media 500b or the external media 500c, with contents enciphered (S35).

[0130]Therefore, use of contents is attained at other terminals, such as a Personal Digital Assistant and a digital television, via these external media 500b or external media 500c.

[0131]When use at Step S31 is not good, namely, when the value of the frequency counter of LT action tag block 620#2 of action and movement is "0", Or at Step S33, when the external media 500b or the external media 500c cannot manage by the secure module Tampa[-proof]-ized in contents by contents control information, the license information treating part 260 ends moving processing. Therefore, copyright is not injured.

[0132]Although this flow chart explained movement, it is applicable also to processing of a copy by changing Step S35 into processing of a copy. Only LT which came to hand a priori may be moved or copied to the external media 500b or the external media 500c.

[0133]As mentioned above, in this system, the distributing server side serves as a subject and the use to each user's contents can be managed. Therefore, the server can grasp the using state of the contents in each user terminal. Even when carrying out service which extends a user's right to acquire, by bonus campaign etc., it can realize only by aiming at upgrade of the user right information data stored in the distributing server.

[0134]On the other hand, based on license information, the user terminal just needs to perform control about reproduction, movement, a duplicate, etc., and can escape the burden of complicated utilization condition management. The alteration of the utilization condition in a terminal, etc. can prevent an illegal use by unifying management of such a utilization condition to the distributing server side.

[0135]According to the contents use management system concerning this embodiment, so that clearly from the above explanation the server 100, User

right-information-data DB120 which memorizes the right information data about the utilization right of the contents which the user who uses the user terminal 200a owns, Based on the demand from said user, LT which is right information data which show a part of utilization right which the user concerned owns is generated, It has the contents information generation part 170 which transmits to the user terminal 200a, and the user terminal 200a is provided with the license information treating part 260 which controls use of contents according to the communications department 210 which receives LT transmitted from the server 100, and the utilization right which received LT shows.

[0136]Therefore, in a terminal unit, it is necessary to manage no utilization rights which a user owns, use of contents can be controlled only by managing some a user's utilization rights which a license ticket shows, and the management burden of a terminal unit can be eased substantially. A server apparatus can be combined with issue of a license ticket, and the using state of the contents in each terminal unit can be grasped, Even when the copy of contents, etc. are performed by the terminal unit, it can be detected by asking a server apparatus copy permission to what kind of medium it was copied when, and pursuit of contents is attained. Since the utilization right which a user owns with a server apparatus is held, Even when the accumulation means (HDD) of a terminal unit crashes, a user's utilization condition etc. can be restored easily, The service which extends a utilization condition which carries out service which is referred to as making reproduction frequency of the utilization condition of contents automatic +1, the addition of a utilization condition, etc. can be processed easily. Since the contents utilization control means of a terminal unit controls use of said contents according to the utilization right which the received license ticket shows, contents unrestricted use with a terminal unit can be prevented certainly.

[0137]The contents which are not enciphered by contents DB140 in the above-mentioned embodiment are accumulated, Although contents were enciphered and distributed at the time of content purchase (drawing 7, S5), contents may be enciphered with a contents key a priori by the server 100, and it may accumulate in contents DB140. In this case, when the purchase request from a user is received, the contents enciphered as it was can be distributed and mitigation of the load of a server and mitigation of a user's waiting time are attained.

[0138]Although the above-mentioned embodiment explained the case where contents and LT were transmitted by communication, it is also possible to transmit contents or LT by broadcast. If it distributes to the user terminal or contents and LT are

simultaneously distributed to beforehand [of contents use of a user's license information] by broadcast in this case, It becomes possible to use the contents which received immediately, and improvement in the response of contents utilization time can be aimed at. The communications processing of contents utilization time can be lost and mitigation of the load of a distributing server can be aimed at.

[0139]Although SAC was formed between server terminals and encryption processing of LT by the contents information encryption section 175 was performed in the above-mentioned embodiment, encryption processing of LT by the contents information encryption section 175 may be omitted.

[0140]When acquiring license information from a server and license information is not enciphered, When LT is stored in the LT accumulating part 245, in order to prevent disclosure of a contents key, an unjust alteration, and the illegal use by other users, it may encipher and store for information peculiar to users, such as terminal ID (client ID). However, encryption is not required when the LT accumulating part 245 is realized by the Tampa[-proof]-ized hardware.

[0141]What recorded various enciphered content on recording media, such as CD-ROM and DVD-ROM, may be distributed as an appendix of a magazine, and what pleasing may be applied to the gestalt which a user purchases. Or using the distribution course of a broadcast system, the distribution contractor side distributes various contents beforehand, is accumulated by the contents accumulating part 240 in the user terminal 220a, and it may apply to the gestalt that a user purchases what pleasing. When a user performs purchase procedure in these cases, the right corresponding to the contents with which a user is pleased is generated by user right-information-data DB120 in the server 100. Thereby, a user becomes possible [requiring issue of LT of contents utilization time]. Since the cost concerning distribution of contents can be held down as much as possible with such a gestalt, the effect of holding down the prices of the contents themselves is expectable.

[0142]What recorded enciphered content on recording media, such as CD-ROM and DVD-ROM, may be applied to the gestalt sold like the usual package. The user who purchased such a recording medium is carrying out a registration procedure, and the right corresponding to the contents purchased to user right-information-data DB120 in the server 100 is generated. It becomes possible henceforth to carry out LT issue requesting at every contents use.

[0143]In the above-mentioned embodiment, shortly after the user's reproduction request occurred, carried out LT issue requesting, but. When it checks whether the LT accumulating part 245 has an LT and there is an LT, it judges whether it is

refreshable at the LT, and when it will reproduce and there will be no LT if refreshable, it may be made to carry out LT issue requesting for the first time.

[0144]In the above-mentioned embodiment, when the user who does the reproduction request of contents did not have a reproduction right of the contents (Step S14 of drawing 10 is N0), gave the notice of being unreproducible, but. A distributing server may be made to process the additional purchase of the reproduction right as that which obtained a user's comprehension or from which the implicit agreement was obtained, without performing a notice of being unreproducible. In this case, the method which performs additional purchase processing on the basis of an implicit agreement becomes the service referred to as that only a part to have used is charged, and can simplify purchase procedure.

[0145]Although license information explained here the case where it had a good/improper parameter about one reproduction, movement, or a duplicate, The parameter showing either one permission of contents playback or unrestricted permission can be included in license information, or the parameter showing either the disapproval of contents movement or unrestricted permission can also be included. In this case, when permission with unrestricted license information is shown, the license information treating part 260 of the user terminal 200a holds a contents key, and always performs operation which provides a contents key to the contents decoding part 270.

[0146]The utilization condition of various contents can be set up by combining two or more propriety information by license information. For example, the processing called Check-in/Check-out is realizable by distributing only reproduction propriety information and move propriety information, and combining these. When Check-in/Check-out makes the duplicate of contents, if it is only reproduced, there is not and it is a reproduction good, and that movement is improper (a duplicate is naturally impossible) and the thing which is carrying out, makes the relation between parent contents and child contents, and prevents free movement of child contents. In the case of this license information, the information on Check-in/Check-out will be held with a distributing server, but. It is not a translation which needs the propriety information of special Check-in/Check-out as license information, It can express in the combination of only reproduction and movement as information which manages and distributes a child's (storage medium) relation with parents (server) when Check-in/Check-out by the server side or a receiver. Therefore, the parameters distributed to a user terminal are reduced, it becomes possible to reduce the burden of a user terminal, and the copy prohibition from a child to a grandchild, etc. can

control a generation copy easily.

[0147]Although justification was checked by the LT footer 640, it may be made to include the information for the alteration detection for checking justification in the above-mentioned embodiment in each LT action tag block 620#1 – every 620#n.

[0148]Although the license information (LT) before the distributed use was accumulated in the LT accumulating part 245 of the user terminal 200a in the above-mentioned embodiment, LT may be temporarily accumulated in the external media 500b or the external media 500c.

[0149]When the user terminal 200 moved contents to the external media 500b and 500c, judged whether it would be movable with the user terminal 200a, but. The server 100 judges beforehand whether the external media 500 of a movement destination can process license information, and only when it can process, it may be made to send the license information to which movement of contents is permitted to a user terminal. At this time, a distributing server communicates with a user terminal, acquires the information on the external media of a movement destination, and determines the move propriety of contents.

[0150]. [whether the external media 500a and 500c can process license information and] Or the contents control information which can be processed is possible also for the external media access part 280 of the user terminal 200a attesting the external media 500a and 500c, and judging with the user terminal 200a about something.

[0151]Although contents distribution, fee collection, etc. besides right management were collectively managed by the server 100, it may constitute from an above-mentioned embodiment so that contents distribution and functions, such as fee collection, may be formed separately.

[0152]

[Effect of the Invention]According to the contents use management system concerning this invention, so that clearly from the above explanation. The license ticket issuing means of a server apparatus generates the license ticket which is right information data which show a part of utilization right which the user concerned owns based on the demand from said user, and transmits to said terminal unit. The contents utilization control means of a terminal unit controls use of said contents according to the utilization right which the received license ticket shows.

[0153]For this reason, in a terminal unit, it is necessary to manage no utilization rights which a user owns, use of contents can be controlled only by managing some a user's utilization rights which a license ticket shows, and the management burden of a terminal unit can be eased substantially. A server apparatus can be combined with

issue of a license ticket, and the using state of the contents in each terminal unit can be grasped, Even when the copy of contents, etc. are performed by the terminal unit, it can be detected by asking a server apparatus copy permission to what kind of medium it was copied when, and pursuit of contents is attained. Since the utilization right which a user owns with a server apparatus is held, Even when the accumulation means (HDD) of a terminal unit crashes, a user's utilization condition etc. can be restored easily, The service which extends a utilization condition which carries out service which is referred to as making reproduction frequency of the utilization condition of contents automatic +1, the addition of a utilization condition, etc. can be processed easily. Since the contents utilization control means of a terminal unit controls use of said contents according to the utilization right which the received license ticket shows, contents unrestricted use with a terminal unit can be prevented certainly.

[0154]Therefore, a server can control use of the contents in a user terminal certainly and easily, without hanging a burden on a user terminal.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a figure showing the composition of the whole contents use management system 1 concerning this embodiment.

[Drawing 2]It is a functional block diagram showing the composition of the server 100 and the user terminals 200a-200c which are shown in drawing 1.

[Drawing 3] It is a figure showing the example of composition of the user management table 111 shown in drawing 2.

[Drawing 4] It is a figure showing the example of composition of the user right-information-data management table 121 shown in drawing 2.

[Drawing 5] It is a figure showing the example of composition of the license information shown in drawing 2.

[Drawing 6] It is a figure showing the data format composition of LT generated by the contents information generation part 170.

[Drawing 7] In this system, it is a flow chart which shows the processing performed, respectively by the user terminal 200a and the server 100 in case a user purchases contents.

[Drawing 8] It is a figure showing a content purchase screen (1).

[Drawing 9] It is a figure showing a content purchase screen (2).

[Drawing 10] In this system, it is a flow chart which shows the processing performed, respectively by the user terminal 200a and the server 100 in case a user uses contents.

[Drawing 11] It is a figure showing a use contents selection picture.

[Drawing 12] It is a figure showing a contents utilization request screen.

[Drawing 13] It is a figure showing a relation with change of the logging utilization condition distributed to a user terminal, and the utilization condition managed by a server.

[Drawing 14] It is a figure showing one relation between a utilization condition and the utilization time.

[Drawing 15] In this system, it is a flow chart which shows the processing performed with the user terminal 200a in the case of moving contents or LT to external media.

[Drawing 16] It is a figure showing a move contents selection picture.

[Drawing 17] It is a block diagram showing the composition of the conventional digital-contents distribution system.

[Drawing 18] It is a flow chart which shows the processing at the time of the content purchase of the conventional digital-contents distribution system.

[Drawing 19] It is a flow chart which shows the processing at the time of the contents playback of the conventional digital-contents distribution system.

[Description of Notations]

1 Contents use management system

100 Server

120 User right information data DB

121 User right-information-data management table

160 User right processing part

165 License information generation part

170 Contents information generation part

190,210 Communications department

200a – a 200c user terminal

260 License information treating part

500b, 500c external media

LT License ticket

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2002-342518
(P2002-342518A)

(43)公開日 平成14年11月29日(2002. 11. 29)

(51)Int.Cl. ⁷	識別記号	F I	テ-マコ-ト [*] (参考)
G 0 6 F 17/60	1 4 2	G 0 6 F 17/60	1 4 2 5 B 0 1 7
	3 0 2		3 0 2 E 5 B 0 8 5
	Z E C		Z E C 5 C 0 5 3
12/14	3 1 0	12/14	3 1 0 K 5 C 0 6 4
15/00	3 3 0	15/00	3 3 0 Z

審査請求 未請求 請求項の数31 ○L (全 25 頁) 最終頁に続く

(21)出願番号 特願2002-24695(P2002-24695)
(22)出願日 平成14年 1 月31日(2002. 1. 31)
(31)優先権主張番号 特願2001-27278(P2001-27278)
(32)優先日 平成13年 2 月 2 日(2001. 2. 2)
(33)優先権主張国 日本 (J P)

(71)出願人 000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者 東 吾紀男
大阪府門真市大字門真1006番地 松下電器
産業株式会社内
(72)発明者 村上 弘規
大阪府門真市大字門真1006番地 松下電器
産業株式会社内
(74)代理人 100109210
弁理士 新居 広守

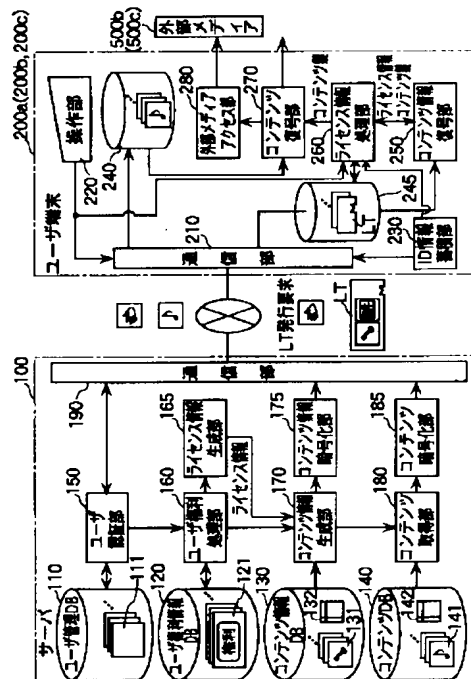
最終頁に続く

(54)【発明の名称】 コンテンツ利用管理システム及びコンテンツ利用管理方法

(57)【要約】

【課題】 ユーザ端末に負担を掛けずに、サーバが、ユーザ端末でのコンテンツの利用を確実に且つ簡単に制御するコンテンツ利用管理システム等を提供する。

【解決手段】 コンテンツ利用管理システムのサーバ100は、ユーザ端末200aを使用するユーザが所有するコンテンツの利用権限に関する権利情報を記憶するユーザ権利情報DB120と、ユーザからの要求に基づいて、当該ユーザが所有する利用権限の一部を示す権利情報であるLTを生成し、ユーザ端末200aに送信するコンテンツ情報生成部170とを備え、ユーザ端末200aは、サーバ100から送信されてきたLTを受信する通信部210と、受信されたLTが示す利用権限に従って、コンテンツの利用を制御するライセンス情報処理部260を備える。



【特許請求の範囲】

【請求項 1】 デジタル著作物であるコンテンツを利用する端末装置と、伝送路を介して前記コンテンツの前記端末装置における利用を管理するサーバ装置とからなるコンテンツ利用管理システムであって、前記サーバ装置は、前記端末装置を使用するユーザが所有するコンテンツの利用権限に関する権利情報を記憶する権利情報記憶手段と、前記ユーザからの要求に基づいて、当該ユーザが所有する利用権限の一部を示す権利情報であるライセンスチケットを生成し、前記端末装置に送信するライセンスチケット発行手段とを備え、前記端末装置は、前記サーバ装置から送信されてきたライセンスチケットを受信する受信手段と、受信されたライセンスチケットが示す利用権限に従って、前記コンテンツの利用を制御するコンテンツ利用制御手段とを備えることを特徴とするコンテンツ利用管理システム。

【請求項 2】 前記ライセンスチケット発行手段は、前記ユーザが所有する利用権限の一部を指定する要求を当該ユーザから取得し、その指定に対応するライセンスチケットを生成し、前記端末装置に送信することを特徴とする請求項 1 記載のコンテンツ利用管理システム。

【請求項 3】 前記ライセンスチケット発行手段は、前記ユーザが所有する利用権限を構成する最小単位の利用権限を示すライセンスチケットを生成し、前記端末装置に送信することを特徴とする請求項 1 記載のコンテンツ利用管理システム。

【請求項 4】 前記ライセンスチケットは、コンテンツの利用に関する 1 以上の可否情報からなることを特徴とする請求項 1 記載のコンテンツ利用管理システム。

【請求項 5】 前記可否情報は、コンテンツの再生、移動及び複製のいずれかの可否を示すことを特徴とする請求項 4 記載のコンテンツ利用管理システム。

【請求項 6】 前記可否情報は、コンテンツの無限回を含む 1 回以上の利用の可又は不可を示すことを特徴とする請求項 4 記載のコンテンツ利用管理システム。

【請求項 7】 前記ライセンスチケット発行手段は、前記ライセンスチケットを暗号化した後に、前記端末装置に送信し、前記端末装置は、さらに、前記受信手段によって受信されたライセンスチケットを復号化する復号化手段を備え、前記コンテンツ利用制御手段は、復号化されたライセンスチケットが示す利用権限に従って、前記コンテンツの利用を制御することを特徴とする請求項 1 記載のコンテンツ利用管理システム。

【請求項 8】 前記復号化手段及びコンテンツ利用制御

手段は、耐タンパ化されたセキュリティモジュールであることを特徴とする請求項 7 記載のコンテンツ利用管理システム。

【請求項 9】 前記ライセンスチケットには、当該ライセンスチケットの内容が改ざんされたか否かを検出するための検出情報が含まれていることを特徴とする請求項 1 記載のコンテンツ利用管理システム。

【請求項 10】 前記コンテンツ利用制御手段は、コンテンツが利用された後に、前記ライセンスチケットが更なるコンテンツの利用を許容しているか否かを判断し、許容していない場合に、当該ライセンスチケットを無効化することを特徴とする請求項 1 記載のコンテンツ利用管理システム。

【請求項 11】 前記端末装置は、さらに着脱可能な外部記録媒体を備え、前記コンテンツ利用制御手段は、コンテンツが利用される前のライセンスチケット及びコンテンツ利用後も更なるコンテンツの利用を許容するライセンスチケットがコンテンツの移動を許容する場合、そのライセンスチケットを前記外部記録媒体に格納することを特徴とする請求項 10 記載のコンテンツ利用管理システム。

【請求項 12】 前記端末装置は、さらに、前記端末装置に接続されている前記外部記録媒体が、前記ライセンスチケットが示す利用権限に従って前記コンテンツの利用を制御する手段を備えているか否かを判定する判定手段を備え、

前記コンテンツ利用制御手段は、前記外部記録媒体が前記制御手段を備えていると判定された場合に、ライセンスチケットを外部記録媒体に格納することを特徴とする請求項 11 記載のコンテンツ利用管理システム。

【請求項 13】 前記コンテンツ利用制御手段は、前記外部記録媒体が前記制御手段を備えていないと判定された場合に、前記ライセンスチケットを異なるフォーマットのコンテンツ制御情報に変換することを特徴とする請求項 12 記載のコンテンツ利用管理システム。

【請求項 14】 前記可否情報は、コンテンツの利用が 1 回行われたと判断する基準となる判定条件を含み、前記コンテンツ利用制御手段は、前記判定条件に基づいてコンテンツの利用を 1 回と判定することを特徴とする請求項 6 記載のコンテンツ利用管理システム。

【請求項 15】 前記判定条件は、コンテンツの利用態様に応じて設定されることを特徴とする請求項 14 記載のコンテンツ利用管理システム。

【請求項 16】 前記判定条件は、コンテンツが再生された時間であり、前記コンテンツ利用制御手段は、コンテンツの前記再生時間に基づいてコンテンツの利用を 1 回と判定することを特徴とする請求項 15 記載のコンテンツ利用管理システム。

【請求項 17】 前記コンテンツ利用制御手段は、前記

再生開始から前記判定条件で示される時間内は、前記1回の利用とみなすことを特徴とする請求項16記載のコンテンツ利用管理システム。

【請求項18】 デジタル著作物であるコンテンツを利用する端末装置に対し、伝送路を介して前記コンテンツの利用を管理するサーバ装置であって、前記端末装置を使用するユーザが所有するコンテンツの利用権限に関する権利情報を記憶する権利情報記憶手段と、

前記ユーザからの要求に基づいて、当該ユーザが所有する利用権限の一部を示す権利情報であるライセンスチケットを生成し、前記端末装置に送信するライセンスチケット発行手段とを備えることを特徴とするサーバ装置。

【請求項19】 前記ライセンスチケット発行手段は、前記ユーザが所有する利用権限の一部を指定する要求を当該ユーザから取得し、その指定に対応するライセンスチケットを生成し、前記端末装置に送信することを特徴とする請求項18記載のサーバ装置。

【請求項20】 前記ライセンスチケット発行手段は、前記ユーザが所有する利用権限を構成する最小単位の利用権限を示すライセンスチケットを生成することを特徴とする請求項18記載のサーバ装置。

【請求項21】 前記サーバ装置は、さらに、前記ユーザからの要求に基づいて、前記端末装置から当該端末装置に接続されている外部記録媒体に関する情報を取得し、前記外部記録媒体が、前記ライセンスチケットが示す利用権限に従って前記コンテンツの利用を制御する手段を備えているか否かを判定する判定手段を備えることを特徴とする請求項18記載のサーバ装置。

【請求項22】 伝送路を介してサーバ装置の許可を受け、デジタル著作物であるコンテンツを利用する端末装置であって、ユーザが所有する利用権限の一部を示す権利情報であるライセンスチケットを前記サーバ装置から受信する受信手段と、受信されたライセンスチケットが示す利用権限に従って、前記コンテンツの利用を制御するコンテンツ利用制御手段とを備えることを特徴とする端末装置。

【請求項23】 前記端末装置は、さらに、前記受信手段によって受信されたライセンスチケットを復号化する復号化手段を備え、前記コンテンツ利用制御手段は、復号化されたライセンスチケットが示す利用権限に従って、前記コンテンツの利用を制御することを特徴とする請求項22記載の端末装置。

【請求項24】 前記コンテンツ利用制御手段は、コンテンツが利用された後に、前記ライセンスチケットが更なるコンテンツの利用を許容しているか否かを判断し、許容していない場合に、当該ライセンスチケットを無効化することを特徴とする請求項22記載の端末装置。

【請求項25】 前記端末装置は、さらに、着脱可能な外部記録媒体を備え、前記コンテンツ利用制御手段は、コンテンツが利用される前のライセンスチケット及びコンテンツ利用後も更なるコンテンツの利用を許容するライセンスチケットがコンテンツの移動を許可する場合、そのライセンスチケットを前記外部記録媒体に格納することを特徴とする請求項24記載の端末装置。

【請求項26】 前記端末装置は、さらに、前記端末装置に接続されている前記外部記録媒体が、前記ライセンスチケットが示す利用権限に従って前記コンテンツの利用を制御する手段を備えているか否かを判定する判定手段を備え、

前記コンテンツ利用制御手段は、前記外部記録媒体が前記制御手段を備えていると判定された場合に、ライセンスチケットを外部記録媒体に格納することを特徴とする請求項25記載の端末装置。

【請求項27】 前記コンテンツ利用制御手段は、前記外部記録媒体が前記制御手段を備えていないと判定された場合に、前記ライセンスチケットを異なるフォーマットのコンテンツ制御情報に変換することを特徴とする請求項26記載の端末装置。

【請求項28】 デジタル著作物であるコンテンツを利用する端末装置と、伝送路を介して前記コンテンツの前記端末装置における利用を管理するサーバ装置とからなるシステムにおけるコンテンツ利用管理方法であって、前記サーバ装置は、

前記端末装置を使用するユーザが所有するコンテンツの利用権限に関する権利情報を記憶する権利情報記憶ステップと、

前記ユーザからの要求に基づいて、当該ユーザが所有する利用権限の一部を示す権利情報であるライセンスチケットを生成し、前記端末装置に送信するライセンスチケット発行ステップとを含み、

前記端末装置は、前記サーバ装置から送信されてきたライセンスチケットを受信する受信ステップと、

受信されたライセンスチケットが示す利用権限に従って、前記コンテンツの利用を制御するコンテンツ利用制御ステップとを含むことを特徴とするコンテンツ利用管理方法。

【請求項29】 前記ライセンスチケット発行ステップでは、前記ユーザが所有する利用権限の一部を指定する要求を当該ユーザから取得し、その指定に対応するライセンスチケットを生成し、前記端末装置に送信することを特徴とする請求項28記載のコンテンツ利用管理方法。

【請求項30】 デジタル著作物であるコンテンツを利用する端末装置と、伝送路を介して前記コンテンツの前記端末装置における利用を管理するサーバ装置とからな

10

20

30

40

50

るコンテンツ利用管理システムにおけるサーバ装置のためのプログラムであって、
請求項18～21のいずれか1項に記載のサーバ装置が備える手段としてコンピュータを機能させるプログラム。

【請求項31】 デジタル著作物であるコンテンツを利用する端末装置と、伝送路を介して前記コンテンツの前記端末装置における利用を管理するサーバ装置とからなるコンテンツ利用管理システムにおける端末装置のためのプログラムであって、
請求項22～27のいずれか1項に記載の端末装置が備える手段としてコンピュータを機能させるプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、通信や放送などで配信された音楽や映像などのデジタルコンテンツ利用を管理するシステム及び方法に関し、特に、コンテンツの再生回数などを制限するコンテンツの権利管理及び利用制御を、確実に且つ簡単に実施できるようにしたものである。

【0002】

【従来の技術】近年、音楽や映像、ゲームなどのデジタル著作物をインターネットやデジタル放送などで配信するシステムが開発され、その一部は、実用化の段階を迎えている。また、これらのコンテンツの配信に当たり、著作権保護等の観点から、配信したコンテンツの再生回数や移動、複製などを制限するコンテンツの権利管理及び利用制御の方式（DRM: Digital Rights Management）が併せて検討されている。

【0003】従来のデジタルコンテンツ配信システムでは、特開2000-48076号公報や、特開2000-293439号公報に見られるように、各ユーザのコンテンツに対する利用条件を、コンテンツと共に受信側に配信して、全てユーザ端末側で管理するようにモデル化されている。

【0004】例えば、あるユーザが、映画“Matrix”について3回視聴する権利を購入する場合には、ユーザ端末は、配信サーバから通信経由で、映画“Matrix”のコンテンツとともに、「Matrixを3回視聴可能」であることを示す利用条件を受信し、コンテンツの再生を利用条件に従って管理する。

【0005】配信サーバは、ユーザ端末に上記利用条件を配信した以降は、ユーザの利用条件に関与しない。ユーザ端末が蓄積したコンテンツを再生して“Matrix”を視聴する場合には、1回視聴する毎にユーザ端末が管理する利用条件を1ずつ減じる処理が行われ、視聴可能回数が0になった時点で、視聴を不許可とする処理が行われる。

【0006】図17は、従来のデジタルコンテンツ配信

システムの構成を示している。

【0007】配信サーバ1000は、会員登録したユーザのID情報などを蓄積するユーザ管理データベース1001と、コンテンツを暗号化するコンテンツ鍵及びコンテンツの利用条件を蓄積するコンテンツ情報データベース1003と、コンテンツを蓄積するコンテンツデータベース1006と、ユーザ認証を行うユーザ認証部1002と、コンテンツの利用条件やコンテンツ鍵の情報を含むコンテンツ情報を生成するコンテンツ情報生成部1004と、コンテンツ情報をユーザID等のユーザの固有情報で暗号化するコンテンツ情報暗号化部1005と、コンテンツデータベース1006から指定されたコンテンツを取得するコンテンツ取得部1007と、コンテンツをコンテンツ鍵で暗号化するコンテンツ暗号化部1008と、ユーザ端末2000との通信部1009とを備えている。

【0008】一方、ユーザ端末2000は、配信サーバ1000との間で通信を行う通信部2001と、ID情報を蓄積するID情報蓄積部2002と、暗号化されたコンテンツを蓄積する蓄積部2003（HDD）と、受信したコンテンツ情報からコンテンツ鍵と利用条件とを復号するコンテンツ情報復号部2006と、コンテンツの利用条件及びコンテンツ鍵を管理する利用条件管理部2007と、コンテンツ再生時の利用条件の処理を行う利用条件処理部2008と、利用条件を満たすときに利用条件処理部2008から取得したコンテンツ鍵でコンテンツを復号するコンテンツ復号部2005と、コンテンツを外部メディア5000に出力する外部メディアアクセス部2004とを備えている。

【0009】図18は、このデジタルコンテンツ配信システムにおいて、ユーザ端末2000が配信サーバ1000からコンテンツを購入するときの処理フローを示している。

【0010】ユーザのコンテンツ購入要求があると、ユーザ端末2000の通信部2001は、ID情報蓄積部2002に蓄積されたユーザ端末2000のID情報を取得し、このID情報とコンテンツ購入要求とを配信サーバ1000に送信する（S1001）。

【0011】この情報を配信サーバ1000の通信部1009を通じて受信したユーザ認証部1002は、受信したID情報をユーザ管理データベース1001に蓄積されているID情報と照合してユーザ認証を行った後、コンテンツ購入要求をコンテンツ情報生成部1004に渡す（S1002）。

【0012】コンテンツ情報生成部1004は、コンテンツ購入に対する課金処理を行い、コンテンツ情報データベース1003から購入コンテンツの利用条件やコンテンツ鍵の情報を取得し、コンテンツ鍵を購入コンテンツの情報とともにコンテンツ取得部1007に渡す。また、利用条件とコンテンツ鍵の情報とを含むコンテンツ

10

20

30

40

50

情報を生成してコンテンツ情報暗号化部1005に渡し、コンテンツ情報暗号化部1005は、コンテンツ情報を暗号化する(S1003)。

【0013】コンテンツ取得部1007は、コンテンツデータベース1006から該当するコンテンツを取得し、コンテンツ暗号化部1008は、このコンテンツをコンテンツ鍵で暗号化する(S1004)。

【0014】配信サーバ1000の通信部1009は、暗号化されたコンテンツと、暗号化されたコンテンツ情報とをユーザ端末2000に送信する。

【0015】ユーザ端末2000の通信部2001は、暗号化されたコンテンツと、コンテンツ鍵及び利用条件の情報を含む暗号化されたコンテンツ情報を受信し(S1005)、コンテンツを蓄積部2003に送って蓄積する(S1006)。

【0016】また、コンテンツ情報をコンテンツ情報復号部2006に送る。コンテンツ情報復号部2006は、暗号化されているコンテンツ情報を復号化し、利用条件とコンテンツ鍵を取り出して利用条件管理部2007に蓄積する(S1007)。

【0017】図19は、このデジタルコンテンツ配信システムにおいて、ユーザ端末2000がコンテンツを再生するときの処理フローを示している。

【0018】ユーザのコンテンツ再生要求があると、利用条件処理部2008は、利用条件管理部2007に管理されている該当するコンテンツの利用条件及びコンテンツ鍵を取得し(S2001)、利用条件の再生回数(再生を許容する回数)をチェックする(S2002)。

【0019】再生回数が0より大きいときは(S2003)、利用条件の再生回数をデクリメントして(S2004)、利用条件及びコンテンツ鍵を利用条件管理部2007に蓄積する(S2005)。

【0020】コンテンツ復号部2005は、蓄積部2003から該当するコンテンツを取得し(S2006)、利用条件処理部2008から渡されたコンテンツ鍵を用いてコンテンツを復号し、コンテンツを再生する(S2007)。また、ステップS2003において、再生回数が0より大きくないときは、再生処理を終了する。

【0021】再生されたコンテンツの映像/音声は、コンテンツ復号部2005からTV等のモニターに出力される。また、コンテンツを外部メディア5000に移動したり、複製したりする場合は、コンテンツの映像/音声外部メディアアクセス部2004を介して外部メディア5000に出力される。

【0022】なお、秘密情報の漏洩を防止するため、秘密情報を扱うID情報蓄積部2002、コンテンツ情報復号部2006及び利用条件管理部2007は、通常、ICカード等のセキュリティモジュールに設置され、このセキュリティモジュールがユーザ端末2000に装着

される。

【0023】この場合、利用条件管理部2007から利用条件処理部2008に利用条件やコンテンツ鍵の情報を送るとき、これらの情報は暗号化されてセキュリティモジュールから出力され、利用条件処理部2008は、これらの情報を復号化して使用する。また、利用条件処理部2008が更新した利用条件を利用条件管理部2007に蓄積する際にも、再暗号化されてセキュリティモジュールに送出される。

10 【0024】従来のデジタルコンテンツ配信システムでは、こうした方式で、各ユーザのコンテンツに対する利用条件がユーザ端末側で管理されている。

【0025】

【発明が解決しようとする課題】しかしながら、各ユーザの利用条件をユーザ端末で管理する場合には、以下のような問題点がある。

(1) ユーザ端末での複雑な利用条件管理が必要であり、ユーザ端末の機能が肥大化する可能性がある。

20 (2) 配信サーバは、配信したコンテンツの利用・権利管理処理に全く関知しないため、ユーザ端末でコンテンツのコピーなどが行われた場合でも、コンテンツを追跡し、何時どのような媒体にコピーされたかを検知することができない。

(3) ユーザ端末の蓄積手段(HDD)がクラッシュした時に、ユーザの利用条件などの復旧が困難である(ユーザ端末以外でその情報を保持しているものが無いため)。

(4) 新規コンテンツを購入すると既購入コンテンツの利用条件の再生回数を自動的に+1する、と云うようなサービスを実施したり、新たな利用条件の追加などを行う場合に、配信サーバ及びユーザ端末の両方のハード、ソフトの変更が必要となる。そのため、こうした利用条件を拡張するサービスや利用条件の追加などの処理が実際上難しい。

【0026】また、各ユーザの利用条件を全て配信サーバ側で管理し、ユーザ端末は、利用条件の制御を行わず、視聴の都度、通信経由でコンテンツ自体(あるいは、コンテンツが暗号化されている場合には、コンテンツ鍵のみでも可)を配信サーバから取得するモデルも考えられるが、この場合には次のような問題点がある。

(5) ユーザ端末にコンテンツを渡した後は、このコンテンツに対する利用制御は行われなため、ユーザ端末では、取得したコンテンツを無制限に利用(特に、再生)することが可能になる。

【0027】本発明は、こうした従来の問題点を解決するものであり、ユーザ端末に負担を掛けずに、サーバが、ユーザ端末でのコンテンツの利用を確実に且つ簡単に制御するコンテンツ利用管理システム、コンテンツ利用管理方法等を提供することを目的としている。

50 【0028】

【課題を解決するための手段】上記目的を達成するために、本発明に係るコンテンツ利用管理システムは、デジタル著作物であるコンテンツを利用する端末装置と、前記コンテンツの前記端末装置における利用を伝送路を介して管理するサーバ装置とからなるコンテンツ利用管理システムであって、前記サーバ装置は、前記端末装置を使用するユーザが所有するコンテンツの利用権限に関する権利情報を記憶する権利情報記憶手段と、前記ユーザからの要求に基づいて、当該ユーザが所有する利用権限の一部を示す権利情報であるライセンスチケットを生成し、前記端末装置に送信するライセンスチケット発行手段とを備え、前記端末装置は、前記サーバ装置から送信されてきたライセンスチケットを受信する受信手段と、受信されたライセンスチケットが示す利用権限に従って、前記コンテンツの利用を制御するコンテンツ利用制御手段を備えることを特徴とする。

【0029】なお、この明細書において、コンテンツの「利用」は、コンテンツの「再生」「移動」「複製」や、電子書籍のコンテンツの「印刷」など、コンテンツを使用する全ての操作は含み、さらに、これらの操作の事前行為として、「ライセンス情報」をダウンロードすること（ライセンスチケットを予めダウンロードすること）も含むものとする。

【0030】ここで、前記ライセンスチケット発行手段は、前記ユーザが所有する利用権限の一部を指定する要求を当該ユーザから取得し、その指定に対応するライセンスチケットを生成し、前記端末装置に送信したり、前記ユーザが所有する利用権限を構成する最小単位の利用権限を示すライセンスチケットを生成し、前記端末装置に送信したりすることを特徴とすることもできる。この構成によれば、各端末装置でのコンテンツの利用状況をきめ細かく把握したり、各端末装置での利用権限の管理負荷を最小限にしたりすることができる。

【0031】また、前記ライセンスチケットには、当該ライセンスチケットの内容が改ざんされたか否かを検出するための検出情報が含まれる構成とすることもできる。これにより、ライセンスチケットの改ざんを確実に防止することができる。

【0032】なお、本発明は、上記コンテンツ利用管理システムを構成するサーバ装置及び端末装置として実現したり、それらサーバ装置及び端末装置を構成する特徴的な手段をステップとするコンテンツ利用管理方法として実現したり、それらステップをパーソナルコンピュータ等に行わせるプログラムとして実現したりすることもできる。そして、そのプログラムをDVD等の記録媒体やインターネット等の伝送媒体を介して広く流通させることができるのは言うまでもない。

【0033】

【発明の実施の形態】以下、本発明の実施の形態について、図面を用いて詳細に説明する。図1は、本実施の形

態に係るコンテンツ利用管理システム1の全体の構成を示す図である。

【0034】このコンテンツ利用管理システム1は、音楽や、映画、書籍など、デジタル化されたコンテンツを購入したユーザに対して付与されるコンテンツ毎の利用権利（ライセンス）をセンタ側が主体となって動的に管理し、コンテンツを利用するためのライセンスチケット（以下、「LT」とも記す。）をユーザの要求に基づいて配信し、LTに含まれる利用条件の範囲内でコンテンツを利用できるようにすることで、コンテンツの著作権を保護するシステムであり、センタに配設されるサーバ100と、コンテンツを利用するユーザが使用するユーザ端末200a～200cと、これらを接続する通信ネットワーク300とから構成される。

【0035】サーバ100は、ワークステーション等のコンピュータであり、ユーザ管理サーバ、コンテンツ配信サーバ、課金サーバ、ライセンス管理サーバとして機能する。具体的には、サーバ100は、本システム1に加入したユーザや、そのユーザが所有する端末を管理したり、ユーザ端末200a～200cなどからコンテンツの購入を受け付けたり、ユーザ端末200a～200c等からのライセンスチケット発行要求（以下、「LT発行要求」とも記す。）を受け付けるWebページを持ち、ユーザ端末200a～200cからのコンテンツ購入要求に応じて課金し、暗号化されたコンテンツをユーザ端末200a～200cに配信したり、LT発行要求に応じて暗号化されたコンテンツをユーザ端末200a～200cで利用するためのLTを配信したりする。このLTは、暗号化されたコンテンツを復号化するためのコンテンツ鍵と、コンテンツについてユーザに付与された利用権利（ライセンス）の中からその一部を切り出した切り出し利用条件とを含む。

【0036】ユーザ端末200a～200cは、パーソナルコンピュータ、携帯情報端末、デジタルテレビ等のコンピュータ装置であり、サーバ100に対するクライアントとして機能する。具体的には、ユーザ端末200a～200cは、ユーザの操作に応じて、インターネットブラウザソフト等のツールを用いてサーバ100のWebページにアクセスし、コンテンツ購入要求を送信してコンテンツの配信を受けたり、コンテンツの利用に当たってLT発行要求を送信してLTを受け取り、LTの切り出し利用条件の範囲でコンテンツを再生したりする。

【0037】なお、ユーザ端末200aには、ユーザ端末200b用の外部メディア500b（例えば、SDカード）や、ユーザ端末200c用の外部メディア500c（例えば、ICカード）を装着することができ、ユーザ端末200aが保持するコンテンツやLTを外部メディア500b、500cに複製したり、移動したりし、ユーザ端末200b、200cでコンテンツを再生する

ことができるように構成されている。

【0038】通信ネットワーク300は、インターネット、CATV等の有線や、デジタル放送等の無線による通信媒体である。

【0039】図2は、図1に示されるサーバ100及びユーザ端末200a～200cの構成を示す機能ブロック図である。なお、ユーザ端末200a～200cの機能構成については同一であるので、ユーザ端末200aをその代表として図示されている。また、本図には通信ネットワーク300も併せて示されている。

【0040】サーバ100は、大きく分けて、ハードディスク等に格納されたデータファイル等によって実現されるデータ部（ユーザ管理DB110、ユーザ権利情報DB120、コンテンツ情報DB130、コンテンツDB140）と、CPU、RAM、ROM等のハードウェア及びCPUにより実行されるプログラム等によって実現される処理部（ユーザ認証部150、ユーザ権利処理部160、ライセンス情報生成部165、コンテンツ情報生成部170、コンテンツ情報暗号化部175、コンテンツ取得部180、コンテンツ暗号化部185、通信部190）とからなる。

【0041】ユーザ管理DB110は、このコンテンツ利用管理システム1に会員登録したユーザのユーザ情報などを蓄積する。具体的には、ユーザ管理DB110は、ユーザの権利を管理するために、ユーザ端末毎に割り当てられるユニークなクライアントID（端末ID）を用い、ユーザIDを含むユーザ情報と対応付けて管理するものであって、会員登録したユーザが所有するユーザ端末のクライアントIDと、そのユーザに対して付与された固有のID情報（ユーザID）と、そのユーザのユーザ情報などを登録・管理するためのユーザ管理テーブル111を複数記憶する記憶部である。

【0042】ユーザ権利情報DB120は、コンテンツに対するユーザの権利情報（ライセンス）を蓄積する。具体的には、ユーザ権利情報DB120は、ユーザが購入したコンテンツや、そのコンテンツに対してユーザが有する利用権（ライセンス）の残存情報を利用の態様（例えば、再生、移動、複写、印刷、利用期間等）毎に管理したりするためのユーザ権利情報管理テーブル121を複数記憶する記憶部である。

【0043】コンテンツ情報DB130は、コンテンツの関連情報（コンテンツ鍵など）を蓄積する。具体的には、コンテンツ情報DB130は、コンテンツを暗号化するための複数のコンテンツ鍵131と、そのコンテンツ鍵131とコンテンツIDとの対応関係を記録したコンテンツ鍵テーブル132等とを保持する。

【0044】コンテンツDB140は、コンテンツを蓄積する。具体的には、コンテンツDB140は、複数のコンテンツ141と、そのコンテンツとコンテンツIDとの対応関係を記録したコンテンツテーブル142とを

蓄積して保持する。

【0045】ユーザ認証部150は、ユーザ認証を行う。具体的には、ユーザ認証部150は、ユーザ端末200a～200cから受け取ったコンテンツ購入要求やLT発行要求に含まれるID情報（クライアントID）から、ユーザ管理テーブル111を用いて、ユーザIDや、サーバで管理される権利を特定する。なお、ユーザ認証部150は、ユーザの住所等が変更されたような場合にはユーザ管理テーブル111のユーザ情報を更新したり、ユーザの端末装置が購入されたような場合にはユーザ管理テーブル111にクライアントIDを追加したりする。

【0046】ユーザ権利処理部160は、購入要求に応じてコンテンツに対するユーザの権利情報の登録を行ったり、利用要求に応じて権利情報の更新を行ったりする。具体的には、ユーザ権利処理部160は、コンテンツ購入要求に応じて課金処理を実行した上で、そのユーザの権利をユーザ権利情報DB120のユーザ権利情報管理テーブル121に登録したりする。

【0047】なお、課金処理自体は本発明の本質ではないので、課金処理を実行する部分は図には記載してはいない。また、ユーザの権利の登録の際には、サーバで管理されるユーザの権利情報であるUR-Us（Usage Rule for User on server）としてコンテンツ提供者が設定した初期値を付与する。また、ユーザ権利処理部160は、LT発行要求があると、その時点の権利情報UR-Usから要求された分の利用権UR-Uc（Usage Rule for User on client）をユーザに切り出すことができるか否か確認し、確認されると要求された利用権UR-Ucをライセンス情報生成部165に渡すと共に、サーバで管理する権利情報UR-Usを切り出し分UR-Ucだけデクリメントした内容に更新する。また、ユーザ権利処理部160は、コンテンツ提供者から権利情報の変更の通知、例えば、コンテンツ購入者へのサービスで利用回数を増やしたり、利用期間を延長したりする通知があった場合、各コンテンツ購入者のライセンス情報を一律に更新する。

【0048】ライセンス情報生成部165は、リクエストされたコンテンツの利用権、ライセンス情報を生成する。

【0049】コンテンツ情報生成部170は、コンテンツ情報DB130からコンテンツ鍵を取得したり、ライセンス情報生成部165から渡されたライセンス情報や取得したコンテンツ鍵の情報を含むコンテンツ情報（LT）を生成する。具体的には、コンテンツ情報生成部170は、コンテンツ情報DB130にアクセスしてコンテンツ鍵テーブル132を用いてコンテンツIDに対応するコンテンツ鍵131を取得したり、このコンテンツ鍵とライセンス情報生成部165から渡されたライセン

10

20

30

40

50

ス情報、切り出し利用条件（U R - U c）とを含めた L T を生成したりする。

【0050】コンテンツ情報暗号化部175は、コンテンツ情報を暗号化する。具体的には、コンテンツ情報暗号化部175は、L T のコンテンツ鍵、及びフッタが付加されている場合にはこのフッタを必要に応じて、暗号化する。この暗号化は、例えば、L T 発行要求を発したユーザ端末200a～200cの端末ID（クライアントID）で暗号化される。このようにクライアントIDで暗号化すると、L T をそのクライアントIDを有するユーザ端末にバインドすることができる。

【0051】なお、公開鍵暗号方式を用い、ユーザの公開鍵で暗号化してもよい。また、サーバと端末で共有された秘密鍵を用いて暗号化してもよい。

【0052】また、サーバ100、ユーザ端末200a～200c間で、例えばSSL（Secure Sockets Layer）などによる相互認証形式でSAC（Secure Authenticated Channel：認証付き安全な通信路）が形成され、サーバと端末間でセキュアな通信路が確保される場合には、ライセンス情報の暗号化は任意である（必須ではない）。ただし、この実施の形態では、サーバ端末間でSACを形成すると共に、コンテンツ情報暗号化部175によるL T の暗号化処理を実行するものとして説明する。

【0053】コンテンツ取得部180は、指定されたコンテンツをコンテンツDB140から取得する。具体的には、コンテンツ取得部180は、コンテンツDB140のコンテンツテーブル142を参照し、コンテンツIDに対応するコンテンツ141を取得し、コンテンツ暗号化部185に渡す。

【0054】コンテンツ暗号化部185は、コンテンツを暗号化する。具体的には、コンテンツ暗号化部185は、コンテンツ暗号化部185から渡されたコンテンツを、暗号化する。この暗号化は、コンテンツ鍵で暗号化される。

【0055】通信部190は、ユーザ端末200と通信する。具体的には、通信部190は、通信ネットワーク300を介してユーザ端末200a～200cと通信するWebページに記述されるスクリプトやプログラム等によって実現される通信インターフェースであって、ユーザ端末200a～200cから送信されてきたコマンドやメッセージを解析したり、その結果に応じてユーザ認証部150に処理を依頼したり、コンテンツ暗号化部185から渡されたコンテンツをユーザ端末200a～200cに配信したり、コンテンツ情報暗号化部175から渡されたL T をユーザ端末200a～200cに配信したり、端末との間でSACを形成したりする。

【0056】一方、ユーザ端末200は、通信部210と、操作部220と、ID情報蓄積部230と、コンテンツ蓄積部240と、L T 蓄積部245と、コンテンツ

情報復号部250と、ライセンス情報処理部260と、コンテンツ復号部270と、外部メディアアクセス部280とを備えている。

【0057】通信部210は、サーバ100との間で通信を行う。具体的には、通信部210は、ブラウザソフト等に従って通信ネットワーク300を介してサーバ100と通信する通信インターフェースであり、操作部220からの依頼に応じてコンテンツ購入要求や、L T 発行要求のメッセージを送信したり、サーバ100から送信されてきたコンテンツをコンテンツ蓄積部240に格納したり、L T をL T 蓄積部245に格納したり、サーバ100の通信部190との間でSACを形成したりする。

【0058】操作部220は、ユーザの操作を受け付けたり、サーバ100が提供するWebページを表示したりするユーザインターフェースである。

【0059】ID情報蓄積部230は、その端末のID情報（クライアントID）を蓄積する。具体的には、ID情報蓄積部230は、各端末毎に予め埋め込まれた固有のクライアントIDを蓄積保持する。また、ID情報蓄積部230は、L T を暗号化するための公開鍵暗号方式の公開鍵と秘密鍵、あるいは、共通鍵暗号方式の暗号鍵を保持してもよい。

【0060】コンテンツ蓄積部240は、例えば、HDD等で構成され、暗号化されたコンテンツを蓄積する。L T 蓄積部245は、通信部210から送られてきたL T を蓄積する。

【0061】コンテンツ情報復号部250は、受信したコンテンツ情報（L T）からコンテンツ鍵とライセンス情報とを復号する。具体的には、コンテンツ情報復号部250は、L T 蓄積部245に蓄積されているL T に含まれるコンテンツ鍵等をクライアントIDや、公開鍵暗号方式の秘密鍵、あるいは共通暗号方式の秘密鍵で復号化する。

【0062】ライセンス情報処理部260は、ライセンス情報に基づいてコンテンツ鍵の使用の可否を識別する。具体的には、ライセンス情報処理部260は、再生可能かどうか判断し、再生可能であればコンテンツ鍵をコンテンツ復号部270に渡し、コンテンツ復号部270によるコンテンツ再生処理において切り出し利用条件が守られるように監視する。

【0063】コンテンツ復号部270は、ライセンス情報処理部260から取得したコンテンツ鍵で暗号化されたコンテンツを復号化する。具体的には、コンテンツ復号部270は、暗号化されたコンテンツをライセンス情報処理部260からもらったコンテンツ鍵で復号化し、ライセンス情報処理部260による管理下でコンテンツを再生する。

【0064】外部メディアアクセス部280は、コンテンツ及びL T のいずれか一方、あるいは両方を、外部メ

ディア500bあるいは外部メディア500cに出力する。

【0065】なお、上記のID情報蓄積部230、LT蓄積部245、コンテンツ情報復号部250、ライセンス情報処理部260は、ハードウェア的に耐タンパ化されたセキュアなモジュール、例えばチップが内蔵されたICカード内に設けられている。この場合、暗号化されたライセンス情報の復号及びライセンス情報の処理はセキュリティモジュールで行なってもよい。ただし、SACが確立された状態でサーバからLTを取得した場合には、ライセンス情報の暗号化は任意であるため、ライセンス情報が暗号化されているときのみ復号化処理を行う。このため、著作権保護上重要な秘密情報、クライアントID、LTに含まれるコンテンツ鍵、利用条件等を外部からアクセスすることを不可能にし、これらの秘密情報を物理的に盗み取ろうとするハードな攻撃に対しても強い設計となっている。ここで、セキュリティモジュールは、耐タンパ化されたソフトウェアでも良い。また、ライセンス情報処理部260は、ユーザ端末のセキュアな部分に設けても良い。

【0066】このように構成されたコンテンツ利用管理システム1では、各ユーザのコンテンツに対する権利情報が、基本的に配信サーバ側で全て管理される。ユーザが購入（あるいは事前契約）したコンテンツは、暗号化された状態でユーザ端末200aのコンテンツ蓄積部240に蓄積される。ユーザ端末200に蓄積されたコンテンツを再生したり、移動や複製を行う場合には、ユーザ端末200からサーバ100にリクエスト、LT発行要求メッセージが出される。サーバ100は、ユーザがリクエストしたコンテンツに対する利用条件（あるいは契約条件）UR-Usを確認し、ユーザの利用権が存在するときは、ユーザに対して「ライセンス情報」とコンテンツ鍵とを含むコンテンツ情報、LTを配信する。ライセンス情報は、コンテンツの再生や、移動、複製などの可否情報で構成され、ユーザ端末は、ライセンス情報で許可されたコンテンツの利用を実行する。

【0067】ユーザが個々のコンテンツを購入等で取得した場合、サーバ100のユーザ権利情報DB120には、ユーザが取得したコンテンツに関する利用条件が管理される。この形式を都度購入型のモデルと云う。このシステムは、その他、サブスクライプ型（事前契約型）のモデルも適用可能である。このサブスクライプ型は、放送で云うティア課金のような形態のものであり、チャンネル契約を行うと該当チャンネルの番組は全て見ることができる、と云うような課金形態である。この場合、ユーザ権利情報DB120には、ユーザ権利情報として契約情報が保持される。

【0068】図3は、図2に示されるユーザ管理テーブル111の構成例を示す図である。

【0069】このユーザ管理テーブル111は、このコ

ンテンツ利用管理システム1に入会したユーザに付与されるユーザIDと、このユーザIDに関連付けられるユーザ情報（「名前」、「住所」、「電話番号1」、「電話番号2」、…、「E-mail1」、「E-mail2」、…）や、このユーザがこのコンテンツ利用管理システム1で使用するユーザ端末に予め付与されるクライアントID（「クライアントID1」、「クライアントID2」、「クライアントID3」、…）等によって構成される。このように構成されたユーザ管理テーブル111によれば、クライアントIDがわかると、そのクライアントIDの端末機器を所有するユーザのユーザIDを特定することができる。

【0070】図4は、図2に示されるユーザ権利情報管理テーブル121の構成例を示す図である。

【0071】このユーザ権利情報管理テーブル121は、クライアントIDまたはユーザIDと、ユーザが購入したコンテンツのコンテンツIDと、コンテンツID毎に設定され、サーバで管理するユーザの利用権（UR-Us）のIDと、ユーザが有する利用権（ライセンス）の利用の態様毎に設定される残存情報などによって構成される。利用の態様毎に設定される残存情報は、各ユーザが購入したコンテンツをあと何回再生できるかや、そのコンテンツをあと何回移動できるか、そのコンテンツをあと何回複製できるか、そのコンテンツをいつまで利用できるか、そのコンテンツをあと何部プリントできるか等をそれぞれ示している。また、残存情報に付属して設定される最長利用時間は、再生処理などにおいてコンテンツを連続して利用できる最大時間を示し、一回判定しきい値はコンテンツの利用を1回と判断する時間を示し、累積利用時間はコンテンツを利用できる累積時間を示している。

【0072】なお、利用権の内容は、コンテンツ提供者やサーバの管理者がコンテンツの属性に応じてコンテンツ毎に初期値が予め定められており、コンテンツ購入時にライセンスの残存情報として初期値が付与される。ここで、同じコンテンツでも、ユーザが取得できる利用条件によって、価格が異なるような販売形態にあっては、購入価格によって異なる初期値であってもよい。そして、このライセンスの残存情報は、ユーザのLT発行要求に応じて切り出される利用条件、ライセンス情報の分ずつ、初期値から順次デクリメントされたり、コンテンツ提供者のサービス提供要求に応じてインクリメントされたりする。

【0073】また、このユーザ権利情報管理テーブル121では、ユーザIDで利用権を管理したが、クライアントIDを用いてユーザの利用権を管理してもよい。

【0074】図5は、図2に示されるライセンス情報の構成例を示す図である。

【0075】このライセンス情報は、切り出された利用権、例えば利用条件の最小限の利用条件要素の情報で生

成され、コンテンツの利用に関する1または複数の可否情報から成り、各可否情報は可否のみを表すパラメータで構成される。ここで、図5中に示される α はアクション、再生に関する可否情報、図5中に示される β はアクション、移動に関する可否情報、図5中に示される γ はアクション、複製に関する可否情報である。これらの可否情報の種類や数は、コンテンツの属性により変化する。

【0076】なお、ここでは、最小限の利用権の場合を説明したが、ユーザが要求する場合には、要求された分切り出し利用権、すなわち、可否だけでなく、可の場合の複数回の利用条件を含めたライセンス情報を生成してもよい。また、図5では、1つのライセンス情報が複数のコンテンツ利用に関する条件で構成される例を示しているが、それぞれ独立の情報としてライセンス情報を構成し、それを複数纏めて1つのコンテンツに対するライセンス情報として扱うことも可能である。

【0077】図6は、コンテンツ情報生成部170により生成されるコンテンツ情報、LTのデータフォーマット構成を示す図である。

【0078】コンテンツ情報生成部170により生成されるLT600は、LTヘッダ610と、ライセンス情報、すなわちコンテンツの操作内容であるアクションと、アクションに対する条件等とを表す1又は複数のLTアクションタグブロック620#1～620#nと、LTコンテンツキータグブロック630と、LTフッタ640とから構成される。

【0079】LTヘッダ610は、このデータがこのコンテンツ利用管理システム1で扱われるライセンスチケットであることを表すLT識別子611と、このコンテンツ利用管理システム1で定められる仕様のバージョンを示すバージョン番号612と、LT全体のデータサイズを示すLTサイズ613と、このLTが関連付けられているコンテンツのコンテンツIDを示すコンテンツID614と、このLTの発行元となったUR-U sのIDを示すUR-U s ID615と、このLTが有効になる日時を示すLT有効期限の開始時刻616と、LTが無効になる日時を示すLT有効期限の終了時刻617と、あるユーザ端末から可搬な外部メディアまたは別のユーザ端末へのコンテンツまたはLTの移動などを許可しているか否かを表すLT移動許可フラグ618と、LTコンテンツキータグブロック630とLTフッタ640に適用される暗号方式(DES, AES等)を示すLT暗号方法619とから構成される。

【0080】LTアクションタグブロック620#1～620#nは、コンテンツに対するアクション内容を特定するIDを示すアクションID621と、コンテンツを連続して操作できる最大時間を示す最長利用時間622と、コンテンツの操作を1回と判断する時間を示す一回判定しきい値623と、このLTでコンテンツを操作

できる最大回数を示す回数カウンタ624と、コンテンツを操作できる累積の操作時間を示す累積利用時間625とから構成される。なお、最長利用時間は、例えばコンテンツが2時間の映画などの場合には、トイレのために一時再生を中断(ポーズ)するようなときでも、映画を最後まで見るように、通常2時間よりも長い値(例えば4時間)に設定される。また、累積利用時間は、最長利用時間よりも厳密な利用制御を行う場合に用いられ、通常2時間よりも長く最長利用時間よりも短い値(例えば3時間)に設定される。

【0081】ここで、一回判定しきい値623が「0」である場合、ユーザ端末200aにおいてコンテンツ操作(利用)を開始した時点で1回と判定され、ある時間が指定がされている場合、その時間に到達すると1回と判定される。また、回数カウンタ624に設定された値はコンテンツの操作を行う毎に減算される。ただし、一回判定しきい値が有効な場合(「0」で無い場合)、コンテンツの連続操作時間が一回判定しきい値の値に到達した時点で減算される。また、連続操作している間には回数カウンタの減算は1度だけ行われる。また、最長利用時間622及び累積利用時間625に設定された時間は、コンテンツの操作時間に応じて減算される。ただし、最長利用時間622に設定された時間はポーズ中も減算されるが、累積利用時間625に設定された時間は、ポーズ中には減算が停止される。なお、回数カウンタ624の値が1以上であれば、可を、0であれば不可を表し、また1であれば最小限の利用条件を表す。したがって、回数カウンタ624を可否情報として用いることもできる。

【0082】LTコンテンツキータグブロック630は、このLTに関連付けられたコンテンツの暗号を解く復号鍵、コンテンツキーが格納される。

【0083】LTフッタ640は、付加するか否か任意のオプションのブロックであり、付加される場合には、LTヘッダ610からLTフッタ640の直前、すなわちLTコンテンツキータグブロック630までの部分の改ざんを防止するため、SHA-1アルゴリズムによるハッシュ値が格納される。

【0084】なお、このLT600ではコンテンツIDをLTヘッダ610に格納したが、コンテンツIDがコンテンツ情報とコンテンツを関連付けるための識別子として設定され、これにより、コンテンツ利用時に取得するコンテンツIDから、コンテンツ情報が特定可能となる重要なものであるため、タグブロックに格納してもよい。

【0085】以上のように構成された本発明の実施の形態におけるコンテンツ利用管理システム1について、以下コンテンツ購入時の動作を図7に示すフローチャートを用いて説明する。

【0086】図7は、このシステムにおいて、ユーザが

10

20

30

40

50

コンテンツを購入する場合のユーザ端末200a及びサーバ100でそれぞれ行われる処理を示すフローチャートである。

【0087】コンテンツを購入する場合、ユーザ端末200aのユーザは、操作部220を操作し、サーバ100のWebページにアクセスし、図8に示されるコンテンツ購入画面(1)を呼び出す。

【0088】このコンテンツ購入画面(1)は、このシステムでネット購入可能なコンテンツのジャンル、「音楽」、「ゲーム」、「電子書籍」、「映画」、…、「有料テレビ番組」の表示と、これらのジャンルを選択するチェックボックスと、「次へ」ボタン、「戻る」ボタン等で構成される。

【0089】購入したいコンテンツのジャンルが、音楽である場合、ユーザは操作部220を操作して、「音楽」に対応するチェックボックスをクリックし、「次へ」ボタンを押下する。これにより図9に示されたコンテンツ購入画面(2)が表示される。

【0090】このコンテンツ購入画面(2)は、ジャンル、音楽に属する曲の「コンテンツID」、「タイトル名」、「権利情報」、「販売価格」の内容と、これらの曲を選択するチェックボックスと、「購入」ボタン、「戻る」ボタン等で構成される。なお、「権利情報」にはコンテンツ提供者が設定したおおもとの利用条件、すなわち残存情報の初期値、再生回数、移動回数、複写回数、利用期間等が示される。購入したい曲が「波乗りジョージ」である場合、ユーザは操作部220を操作して、「波乗りジョージ」に対応するチェックボックスをクリックし、「購入」ボタンを押下し、コンテンツ購入要求を入力する。

【0091】ユーザのコンテンツ購入要求があると、ユーザ端末200aの通信部210は、サーバ100の通信部190との間でSACを形成した後、ID情報蓄積部230に蓄積されたユーザ端末200のID情報(クライアントID)を取得し、このID情報を含むコンテンツ購入要求メッセージをサーバ100に送信する(S1)。このコンテンツ購入要求メッセージは、例えば、コンテンツ購入を表すメッセージID、購入を希望するコンテンツのコンテンツIDと、コンテンツ購入を要求するユーザ端末のクライアントIDなどから構成される。

【0092】ユーザ認証部150は、この情報をサーバ100の通信部190を通じて受信すると、受信したID情報をユーザ管理DB110に蓄積されているID情報と照合してユーザ認証を行った後、コンテンツ購入要求をユーザ権利処理部160に渡す(S2)。具体的には、ユーザ認証部150は、ユーザ管理テーブル111を参照し、クライアントIDからユーザIDを特定した後、コンテンツ購入要求として、ユーザID、コンテンツID等をユーザ権利処理部160に渡す。

【0093】ユーザ権利処理部160は、コンテンツ購入の課金処理を行った後、ユーザ権利情報DB120に、購入コンテンツに対するユーザの権利情報を登録する(S3)。具体的には、ユーザ権利処理部160は、ユーザ権利情報DB120にアクセスし、コンテンツを購入するユーザ(例えば、東□△)用のユーザ権利情報管理テーブル121(図4参照)をユーザID「pana01」から特定する。そして、ユーザ権利処理部160は、ユーザ権利情報管理テーブル121のコンテンツIDの欄に曲1をそれぞれ格納し、各コンテンツID毎のライセンス情報の欄に曲1の権利情報UR-UsのID、「権利情報A」とその内容をそれぞれ格納する。この権利情報Aの内容には、コンテンツ提供者が設定した初期値の残存情報(再生回数、移動回数、複写回数等)が設定される。そして、ユーザ権利処理部160は、コンテンツIDをコンテンツ情報生成部170に渡す。

【0094】コンテンツ情報生成部170は、コンテンツ情報DB130から該当コンテンツの関連情報(コンテンツ鍵など)を取得してコンテンツ取得部180に渡す(S4)。具体的には、コンテンツ情報生成部170は、コンテンツ情報DB130にアクセスし、コンテンツ鍵テーブル132を参照してコンテンツIDに対応するコンテンツ鍵131を取得し、取得したコンテンツ鍵とコンテンツIDとをコンテンツ取得部180に渡す。

【0095】コンテンツ取得部180は、コンテンツDB140から該当コンテンツを取得し、コンテンツ暗号化部185は、このコンテンツをコンテンツ鍵で暗号化する(S5)。具体的には、コンテンツ取得部180は、コンテンツDB140にアクセスし、コンテンツテーブル142を参照してコンテンツIDに対応するコンテンツを取得して、取得したコンテンツと、コンテンツ情報生成部170から受け取ったコンテンツ鍵と、クライアントIDとをコンテンツ暗号化部185に渡す。コンテンツ暗号化部185は、受け取ったコンテンツをコンテンツ鍵で暗号化し、暗号化したコンテンツを通信部190に渡す。サーバ100の通信部190は、暗号化されたコンテンツをユーザ端末200に送信する(S5)。

【0096】ユーザ端末200の通信部210は、暗号化されたコンテンツを受信すると(S6)、コンテンツをコンテンツ蓄積部240に送って蓄積する(S7)。このようなユーザ端末200a及びサーバ100のそれぞれの処理の実行により、コンテンツ購入時のセッションが終了する。

【0097】なお、コンテンツ購入時のセッションでは、ユーザ端末200a-サーバ100間にSACが形成され、共通のセッション鍵で暗号通信が行われるため、コンテンツ購入要求メッセージのネットワーク上での解読を防止することができる。

【0098】図10は、このシステムにおいて、ユーザ

がコンテンツを利用する場合のユーザ端末200a及びサーバ100でそれぞれ行われる処理を示すフローチャートである。

【0099】コンテンツを利用する場合、ユーザ端末200aのユーザは、操作部220を操作し、図11に示される利用コンテンツ選択画面を表示させる。この利用コンテンツ選択画面は、ユーザ端末200aのユーザが購入したコンテンツのタイトル、コンテンツID、あるいは、事前契約したコンテンツについてのライセンスチケットの事前申込み等と、これらのコンテンツについての

のチェックボックス、「次へ」ボタン、「戻る」ボタン等から構成される。

【0100】コンテンツを利用する場合、ユーザは操作部220を操作して再生するコンテンツの利用情報を入力する。具体的には、ユーザは、図11に示される利用コンテンツ選択画面を表示させて、再生を希望するコンテンツ（例えば、波乗りジョージ）のチェックボックスにチェックマークを入力し、「次へ」ボタンをクリックする。そして、図12に示されるコンテンツ利用要求画面を表示させる。コンテンツ利用要求画面は、このコン

テンツで利用可能なアクション、再生、移動、複写と、このアクションを選択するチェックボックス、アクションの回数を入力するテキストボックス、「決定」ボタン、「戻る」ボタン等から構成される。

【0101】ユーザは、利用情報の入力の一環として、操作部220を操作して、選択したコンテンツ（波乗りジョージ）について、必要な要求内容（この例では再生、移動）のチェックボックスにチェックマークを入れ、チェックマークを入れた要求内容のテキストボックスに要求数（この例では、再生について「2」回、移動について「1」回）を入力し、「決定」ボタンをクリックする。

【0102】なお、チェックボックスにチェックマークを入れると、そのテキストボックスにが最小の利用条件として「1」が予め入力される。そして、ユーザが「2」回以上の利用を欲する場合には、欲する回数をテキストボックスに入力すればよい。

【0103】ユーザのコンテンツ再生要求があると、ユーザ端末200の通信部210は、サーバ100の通信部190とSACを形成した後、ID情報蓄積部230に蓄積されたユーザ端末200のID情報（クライアントID）を取得し、このID情報を含むLT発行要求メッセージをサーバ100に送信する（S11）。このLT発行要求メッセージは、例えば、LT発行要求を表すメッセージID、利用対象のコンテンツのコンテンツID（例えば、曲1）と、コンテンツ再生要求、すなわちコンテンツ利用要求の内容を表す要求情報（再生2回、移動1回）と、LT発行を要求するユーザ端末のクライアントID（例えば、nat01）などから構成される。

【0104】この情報をサーバ100の通信部190を通じて受信したユーザ認証部150は、受信したID情報をユーザ管理DB110に蓄積されているID情報と照合してユーザ認証を行った後、ユーザ情報とコンテンツ再生要求とをユーザ権利処理部160に渡す（S12）。具体的には、ユーザ認証部150は、ユーザ管理テーブル111を参照し、クライアントIDからユーザIDを特定した後、ユーザIDと、コンテンツ再生要求として、クライアントID、コンテンツID、要求情報等をユーザ権利処理部160に渡す。

【0105】ユーザ権利処理部160は、ユーザ権利情報DB120に登録されている、リクエストしたコンテンツに対するユーザの権利情報を確認する（S13）。具体的には、ユーザ権利処理部160は、ユーザ権利情報DB120にアクセスし、コンテンツを利用するユーザ（例えば、東口△）用のユーザ権利情報管理テーブル121（図4参照）をユーザID「pana01」から特定する。そして、ユーザ権利処理部160は、ユーザ権利情報管理テーブル121のコンテンツIDの欄、曲1を参照し、曲1の残存情報（UR-U s）に、再生、移動が含まれているか、再生、移動に要求された回数が残っているか等を確認する。

【0106】なお、サブスクライブ型（事前契約型）の場合のユーザの権利情報の確認は、リクエストの有ったコンテンツが、どのサブスクリプション（契約）に含まれるものであるか、及び、ユーザが当該サブスクリプションを有しているか否か、について判定することにより行われる。

【0107】登録した権利情報の中に、リクエストしたコンテンツに対する再生の権利情報が含まれているときは（S14）、ユーザ権利処理部160は、その権利情報に基づいて再生の可否をライセンス情報生成部165に伝え、再生の権利情報の内容を更新（再生可能回数のデクリメント）してユーザ権利情報DB120に格納する（S15）。ライセンス情報生成部165は、ユーザ権利処理部160から伝えられた情報を基にライセンス情報を生成してコンテンツ情報生成部170に渡す（S15）。具体的には、図13に示されるように、ユーザ権利処理部160は、ユーザID「pana01」のコンテンツIDの残存情報、再生回数「10回」、移動回数「2回」、複写回数「3回」を、再生回数「8回」、移動回数「1回」、複写回数「3回」に更新し、すなわち利用条件（UR-U s）を、再生については10回から8回に、移動については3回から2回に減少させ、ライセンス情報生成部165は、再生回数「2回」、移動回数「1回」のライセンス情報をコンテンツ情報生成部170に渡し、LTとしてユーザ端末200aに送らせる。

【0108】なお、サーバ側の判断により、ユーザ端末から要求された利用権利を満たさない利用権利をLTと

して送信することもできる。例えば、ユーザ端末から2回再生の権利を要求された場合でも、1回の再生権利をLTとして送信することで、ビジネス的判断等により、最小限の利用権利を毎回送信するというポリシーを確保することが可能となる。

【0109】コンテンツ情報生成部170は、コンテンツ情報DB130から該当コンテンツのコンテンツ鍵の情報を読み出し、このコンテンツ鍵とライセンス情報とを含むコンテンツ情報(LT)を生成する(S16)。具体的には、コンテンツ情報生成部170は、LTヘッダ610と、アクション、再生で、回数カウンタの値「2」のLTアクションタグブロック620#1と、アクション、移動で、回数カウンタの値「1」のLTアクションタグブロック620#2、LTコンテンツキータグブロック630と、LTフッタ640とからなるLT600を生成する。コンテンツ情報暗号化部175は、このコンテンツ情報を暗号化する(S16)。具体的には、コンテンツ情報暗号化部175は、LTコンテンツキータグブロック630と、LTフッタ640とを暗号化する。

【0110】サーバ100の通信部190は、暗号化されたコンテンツ鍵とライセンス情報とをLTとしてユーザ端末200に送信する。

【0111】なお、ステップS14において、ユーザの権利情報の中に、リクエストしたコンテンツに関する再生の権利情報が含まれていないときは、再生不可レスポンスメッセージがサーバ100からユーザ端末200に送信される。この再生不可レスポンスメッセージは、例えば、LT発行要求メッセージに対するレスポンスであることを表すメッセージIDと、要求に該当するURUUSが存在せず、再生不可であることを表すステータスIDで構成される。

【0112】一方、ユーザ端末200では、コンテンツ情報を受信した通信部210は、LTをLT蓄積部245に格納した後、LTとID情報蓄積部230に格納されたクライアントIDとをコンテンツ情報復号部250に送る(S18)。コンテンツ情報復号部250は、暗号化されたコンテンツ情報(LT)をクライアントIDで復号化してライセンス情報とコンテンツ鍵とをライセンス情報処理部260に渡す(S18)。

【0113】ライセンス情報処理部260は、ライセンス情報の再生可否情報をチェックし(S19)、再生可のときは(S20)、コンテンツ復号部270にコンテンツ鍵を渡す。具体的には、ライセンス情報処理部260は、アクション、再生の回数カウンタが1以上であるか否かをチェックし、1以上である場合に、コンテンツ復号部270にコンテンツ鍵を渡す。コンテンツ復号部270は、コンテンツ蓄積部240からコンテンツを取得して(S21)、コンテンツ鍵でコンテンツを復号してライセンス情報処理部260の切り出し利用条件によ

る管理の下、曲1「波乗りジョージ」を再生する(S22)。

【0114】ところで、アクション、再生のLTアクションタグブロック620#1には、回数カウンタの値のほか、一回判定しきい値、最長利用時間、累積利用時間が含まれている。

【0115】このため、ユーザ端末でのコンテンツの再生について、再生開始から一定時間が経過した場合に1回の再生が行われたものと判断する方式を取り、この一定時間の情報を配信サーバから配信することにより、一定時間を可変することができる。

【0116】また、再生開始時点で1回再生されたものとして、再生開始から一定時間内であれば、同一の再生と見做し、再生を許可すると云う方式を取ることも可能であり、この範囲を示す情報を配信し、1回再生のタイムリミットとすることもできる。

【0117】すなわち、図14に示されるように、一回判定しきい値としてある時間設定しておけば、その時間未満の再生(例えば、頭出し等のプレ再生等)の場合には、その再生は1回とカウントされることはない。そして、一回判定しきい値に達して初めて1回の再生とカウントさせることができる。また、最長利用時間にある時間を設定しておけば、最長利用時間に達するまで、1回の再生権利を消費するだけで、そのコンテンツを断続的に再生させることができるため、再生中に一時停止(ポーズ)ができるといった柔軟な利用形態が実現できる。また、累積利用時間にある時間を設定しておけば、累積利用時間に達するまでコンテンツを累積再生させることができる。したがって、ユーザに対して多様なコンテンツ利用を提供することができる。

【0118】また、こうした再生可能期間の判断方法に関するポリシーを、コンテンツ種別(例えば、映画と音楽と)に応じて変えるようにしても良い。

【0119】なお、サーバ100から再生不可レスポンスメッセージを受けたとき(S17)、及び、ステップS20において、ライセンス情報が再生不可のときは、コンテンツを再生すること無く処理を終了する。ここで、再生不可の通知は、例えば、要求に該当する利用権URUUSが存在しないこと示すステータスコードERROR_URUSで形成されたレスポンスメッセージにより行われる。また、再生回数カウンタの値を「0」としたLTアクションタグブロック620を含むLTで再生不可を通知してもよい。

【0120】また、ライセンス情報がコンテンツの1回の利用だけを規定している場合、ライセンス情報処理部260は、コンテンツを利用した後、このライセンス情報を削除し、あるいは無効であることを示すフラグなどを設定して、ライセンス情報(LT)を無効化する処理を行う。

【0121】なお、ライセンス情報が複数のアクション

10

20

30

40

50

の条件（例えば、再生と移動）を含み、それらを纏めて1つのコンテンツに対するライセンス情報として扱う場合には、当該利用した条件（例えば、再生）のみを無効化する。

【0122】また、サブスクライブ型でも、コンテンツそれぞれには、無制限の利用が認められる場合（例えば、ティア課金）もあれば、利用条件の上限が定められる場合もある（例えば、PPV（Pay Per View）で、月額上限5000円等）。利用条件の上限が有る場合には、ユーザの権利情報の確認の際に、前記契約の判定を行った後、ユーザが当該コンテンツの利用条件を有しているかどうかの判定（都度契約型の判定）を行うことになる。また、ユーザ権利情報DB120は、契約情報のデータベースと利用条件のデータベースとに分離して管理するようにしても良い。

【0123】ここで、このコンテンツ利用管理システム1では、ライセンス情報でコンテンツの移動や複製が“可”であるときは、外部メディアアクセス部280を介して外部メディア500b、500cに、コンテンツと共に権利情報（利用条件）及びコンテンツ鍵を移動することが可能である。このとき権利情報は、外部メディア500b、500cでサポートされているデータ形式に変換した上で移動や複製を行う。また、コンテンツについても、外部メディア500b、500cでサポートされている暗号方式で暗号変換（再暗号化）され、同様にコンテンツ鍵も外部メディア500b、500cでサポートされている暗号方式に対応した暗号鍵に変換される。このように、外部メディアを用いることで、本コンテンツ利用管理システム1とは別のコンテンツ管理方法でコンテンツの著作権保護を図りつつ、コンテンツの利用が可能となる。ただし、外部メディアが本発明のコンテンツ利用管理システム1をサポート可能である場合には、権利情報のデータ変換やコンテンツの暗号変換は不要である。

【0124】図15は、このシステムにおいて、コンテンツまたはLTを外部メディアに移動する場合のユーザ端末200aで行われる処理を示すフローチャートである。

【0125】コンテンツまたはLTを移動する場合、ユーザ端末200aのユーザは、操作部220を操作し、図16に示される移動コンテンツ選択画面を表示させる。この移動コンテンツ選択画面は、ユーザ端末200aのユーザが購入したコンテンツのタイトル、コンテンツID、あるいは、事前に受け取ったライセンスチケット等と、これらのコンテンツ、LTについてのチェックボックス、「決定」ボタン等から構成される。ユーザは、図16に示される利用コンテンツ選択画面を表示させて、移動を希望するコンテンツ（例えば、波乗りジョージ）のチェックボックスにチェックマークを入力し、「決定」ボタンをクリックする。

【0126】ユーザのコンテンツ移動要求があると、ユーザ端末200aのライセンス情報処理部260は、ID情報蓄積部230に格納されたクライアントIDと、LT蓄積部245に蓄積されたLTとをコンテンツ情報復号部250に渡す。コンテンツ情報復号部250は、暗号化されたコンテンツ情報（LT）をクライアントIDで復号化してライセンス情報とコンテンツ鍵とをライセンス情報処理部260に渡す。

【0127】ライセンス情報処理部260は、ライセンス情報の移動可否情報をチェックし、利用可か否か、すなわちアクション、移動のLTアクションタグブロック620#2の回数カウンタの値が1以上（「利用前」または「利用後かつ利用可」の場合）であるか否かを判断する（S31）。利用可であれば（S31でYes）、コンテンツ復号部270、外部メディアアクセス部280を介して外部メディア500bあるいは外部メディア500cがLTを処理可能か否かを判断する（S32）。

【0128】処理可能でなければ（S32でNo）、ライセンス情報処理部260は、利用条件をコンテンツ制御情報に変換した情報にフォーマット変換するか否かを判断する（S33）。すなわち、ライセンス情報処理部260は、外部メディア500bあるいは外部メディア500cがコンテンツ制御情報でコンテンツを耐タンパ化されたセキュアなモジュールで管理できるか否かを判断する。管理できれば、ライセンス情報処理部260は、移動のLTアクションタグブロック620#2をコンテンツ制御情報に変換し（S34）、変換したコンテンツ制御情報とコンテンツ鍵とをコンテンツ復号部270に渡す。コンテンツ復号部270はコンテンツ蓄積部240からコンテンツを取得して、コンテンツ鍵でコンテンツを復号し、復号化されたコンテンツと、ライセンス情報処理部260から渡されたコンテンツ制御情報とを外部メディアアクセス部280に渡す。外部メディアアクセス部280は、コンテンツ復号部270から渡された復号化コンテンツとコンテンツ制御情報とを外部メディア500bあるいは外部メディア500cに移動する（S35）。

【0129】また、ステップS32において処理可能であれば、ライセンス情報処理部260は、LTをコンテンツ復号部270に渡す。コンテンツ復号部270はコンテンツ蓄積部240からコンテンツを取得して、コンテンツ鍵でコンテンツを復号し、復号化されたコンテンツと、ライセンス情報処理部260から渡されたLTとを外部メディアアクセス部280に渡す。外部メディアアクセス部280は、コンテンツ復号部270から渡された復号化コンテンツとLTとを外部メディア500bあるいは外部メディア500cに移動する（S35）。この場合、コンテンツ復号部270は、コンテンツを復号化せずに外部メディアアクセス部280に渡し、外部メディアアクセス部280はコンテンツを暗号化したま

ま外部メディア 500b あるいは外部メディア 500c に移動してもよい (S35)。

【0130】したがって、この外部メディア 500b あるいは外部メディア 500c を介して、携帯情報端末やデジタルテレビなどの他の端末でもコンテンツの利用が可能となる。

【0131】ステップ S31 で利用可でない場合、すなわち、アクション、移動の L T アクションタグブロック 620 #2 の回数カウンタの値が「0」である場合、あるいはステップ S33 で外部メディア 500b あるいは外部メディア 500c がコンテンツ制御情報でコンテンツを耐タンパ化されたセキュアなモジュールで管理できない場合には、ライセンス情報処理部 260 は、移動処理を終了する。したがって、著作権が害されることはない。

【0132】なお、このフローチャートでは移動について説明したが、ステップ S35 を複写の処理に変更することにより、複写の処理にも適用することができる。また、事前に入手した L T だけを外部メディア 500b あるいは外部メディア 500c に移動あるいは複写してもよい。

【0133】以上のように、このシステムでは、各ユーザのコンテンツに対する利用を配信サーバ側が主体となって管理することができる。したがって、サーバは、各ユーザ端末でのコンテンツの利用状況を把握することができる。また、ボーナスキャンペーンなどでユーザの取得済み権利を拡張するサービスを実施する場合でも、配信サーバに格納されたユーザ権利情報のグレードアップを図るだけで実現できる。

【0134】一方、ユーザ端末は、ライセンス情報に基づいて、再生や移動、複製などに関する制御を実行するだけで済み、複雑な利用条件管理の負担を免れることができる。また、こうした利用条件の管理を配信サーバ側に一元化することで、端末での利用条件の改ざん等、不正利用を防止できる。

【0135】以上の説明から明らかなように、本実施の形態に係るコンテンツ利用管理システムによれば、サーバ 100 は、ユーザ端末 200a を使用するユーザが所有するコンテンツの利用権限に関する権利情報を記憶するユーザ権利情報 DB 120 と、前記ユーザからの要求に基づいて、当該ユーザが所有する利用権限の一部を示す権利情報である L T を生成し、ユーザ端末 200a に送信するコンテンツ情報生成部 170 とを備え、ユーザ端末 200a は、サーバ 100 から送信されてきた L T を受信する通信部 210 と、受信された L T が示す利用権限に従って、コンテンツの利用を制御するライセンス情報処理部 260 を備える。

【0136】したがって、端末装置では、ユーザが所有する全ての利用権限を管理する必要はなく、ライセンスチケットが示すユーザの一部の利用権限を管理するだけ

でコンテンツの利用を制御でき、端末装置の管理負担を大幅に軽減することができる。また、サーバ装置は、ライセンスチケットの発行に併せて各端末装置でのコンテンツの利用状況を把握することができ、端末装置でコンテンツのコピーなどが行われた場合でも、サーバ装置にコピー許可の問い合わせを行うことで何時どのような媒体にコピーされたかを検知することができ、コンテンツの追跡が可能になる。また、サーバ装置でユーザが所有する利用権限を保持しているため、端末装置の蓄積手段 (HDD) がクラッシュした時でも、ユーザの利用条件などを容易に復旧でき、また、コンテンツの利用条件の再生回数を自動的に +1 する、と云うようなサービスを実施するような利用条件を拡張するサービスや利用条件の追加などの処理が容易に行える。さらに、端末装置のコンテンツ利用制御手段は受信されたライセンスチケットが示す利用権限に従って、前記コンテンツの利用を制御するので、端末装置でのコンテンツ無制限利用を確実に防止することができる。

【0137】なお、上記実施の形態ではコンテンツ DB 140 に暗号化されていないコンテンツを蓄積し、コンテンツ購入時にコンテンツを暗号化して配信したが (図 7、S5)、サーバ 100 でコンテンツを事前にコンテンツ鍵で暗号化してコンテンツ DB 140 に蓄積しておいてもよい。この場合、ユーザからの購入要求を受けた場合には、そのまま暗号化されたコンテンツを配信することができ、サーバの負荷の軽減及びユーザの待ち時間の軽減が可能となる。

【0138】また、上記実施の形態では、コンテンツ及び L T を通信で伝送する場合について説明したが、放送によりコンテンツまたは L T を伝送することも可能である。また、この場合、ユーザのライセンス情報を、コンテンツ利用の事前にユーザ端末に配信しておく、あるいは放送によりコンテンツと L T とを同時に配信しておけば、受信したコンテンツを直ぐに利用することが可能になり、コンテンツ利用時のレスポンスの向上を図ることができる。また、コンテンツ利用時の通信処理を無くすることができ、配信サーバの負荷の軽減を図ることができる。

【0139】また、上記実施の形態では、サーバー端末間で S A C を形成すると共に、コンテンツ情報暗号化部 175 による L T の暗号化処理を実行したが、コンテンツ情報暗号化部 175 による L T の暗号化処理を省略してもよい。

【0140】また、サーバからライセンス情報を取得する際に、ライセンス情報が暗号化されていない場合には、L T 蓄積部 245 に L T を格納する際に、コンテンツ鍵の露呈、不正な改ざん、他のユーザによる不正利用を防止するため、端末 ID (クライアント ID) などのユーザ固有の情報で暗号化して格納してもよい。ただし、L T 蓄積部 245 が耐タンパ化されたハードウェア

10

20

30

40

50

で実現される場合には、暗号化は必要ではない。

【0141】また、CD-ROM、DVD-ROM等の記録媒体に種々の暗号化コンテンツを記録したものを雑誌の付録として配布し、気に入ったものをユーザが購入する形態に適用してもよい。あるいは、放送系の配信経路を用いて配信業者側が種々のコンテンツをあらかじめ配信し、ユーザ端末220a内のコンテンツ蓄積部240で蓄積しておいて、気に入ったものだけユーザが購入するといった形態に適用してもよい。これらの場合、ユーザが購入手続きを行うことにより、ユーザが気に入ったコンテンツに対応する権利がサーバ100内のユーザ権利情報DB120に生成される。これによりユーザはコンテンツ利用時にLTの発行を要求することが可能となる。このような形態であれば、コンテンツの配信にかかるコストを極力抑えることができるため、コンテンツ自体の価格を抑える効果が期待できる。

【0142】また、CD-ROM、DVD-ROM等の記録媒体に暗号化コンテンツを記録したものを通常のパッケージと同様に販売する形態に適用してもよい。このような記録媒体を購入したユーザは、登録手続きをすることで、サーバ100内のユーザ権利情報DB120に購入したコンテンツに対応する権利が生成される。以後はコンテンツ利用のたびにLT発行要求をすることが可能となる。

【0143】また、上記実施の形態では、ユーザの再生要求があると直ちに、LT発行要求をしたが、LT蓄積部245にLTがあるか否か確認し、LTがあると、そのLTで再生可能か否か判断し、再生可能であれば、再生し、LTが無い場合に、初めてLT発行要求をするようにしてもよい。

【0144】また、上記実施の形態では、コンテンツの再生要求をするユーザが、そのコンテンツの再生権利を有しない場合(図10のステップS14がN0)、再生不可の通知をしたが、配信サーバは、再生不可の通知を行わずに、ユーザの了解を得て、あるいは暗黙の了解が得られたものとして、その再生権利の追加購入の処理を行うようにしてもよい。この場合、暗黙の了解のもとに追加購入処理を行う方式は、利用した分だけ課金されると言うサービスになり、購入手続きを簡略化することができる。

【0145】また、ここでは、ライセンス情報が、1回の再生、移動または複製に関する可/不可のパラメータを有する場合について説明したが、ライセンス情報に、コンテンツ再生の1回のみの許可または無制限の許可のいずれかを表すパラメータを含めたり、コンテンツ移動の不許可または無制限の許可のいずれかを表すパラメータを含めたりすることもできる。この場合、ライセンス情報が無制限の許可を示しているときは、ユーザ端末200aのライセンス情報処理部260がコンテンツ鍵を保持し、コンテンツ復号部270に、常時、コンテンツ

鍵を提供する動作を行う。

【0146】また、ライセンス情報で、複数の可否情報を組み合わせることにより、様々なコンテンツの利用条件を設定することができる。例えば、再生可否情報と、移動可否情報のみを配信し、これらを組み合わせることにより、Check-in/Check-outと云う処理が実現できる。Check-in/Check-outは、コンテンツの複製を作る際に、単に複製するのではなく、再生可、移動不可(当然、複製は不可)とすることで、親コンテンツと子コンテンツの関係を作り、子コンテンツの自由移動を防ぐものである。このライセンス情報の場合、配信サーバでは、Check-in/Check-outの情報は保持することになるが、ライセンス情報としては、特段Check-in/Check-outという可否情報が必要な訳ではなく、Check-in/Check-outしたときの親(サーバ)と子(蓄積メディア)の関係をサーバ側または受信側で管理し、かつ、配信する情報として、再生と移動のみの組み合わせで表現できる。そのため、ユーザ端末に配信するパラメータを削減し、ユーザ端末の負担を減らすことが可能になり、子から孫へのコピー禁止等、ジェネレーションコピーを簡単に制御することができる。

【0147】また、上記実施の形態では、LTフック640で正当性をチェックしたが、各LTアクションタグブロック620#1~620#n毎に、正当性をチェックするための改ざん検出用の情報を含めるようにしても良い。

【0148】また、上記実施の形態では、配信された利用前のライセンス情報(LT)をユーザ端末200aのLT蓄積部245に蓄積したが、LTを外部メディア500bあるいは外部メディア500cに一時的に蓄積してもよい。

【0149】また、ユーザ端末200aがコンテンツを外部メディア500b、500cに移動する場合、ユーザ端末200aで移動可能か判断したが、サーバ100は、移動先の外部メディア500がライセンス情報を処理可能か否かを予め判定し、処理可能であるときのみ、コンテンツの移動を許可するライセンス情報をユーザ端末に送るようにしてもよい。このとき、配信サーバは、ユーザ端末と通信して、移動先の外部メディアの情報を取得し、コンテンツの移動可否を決定する。

【0150】また、外部メディア500a、500cがライセンス情報を処理可能かどうか、あるいは、処理可能なコンテンツ制御情報が何かについては、ユーザ端末200aの外部メディアアクセス部280が、外部メディア500a、500cの認証を行い、ユーザ端末200aで判断することも可能である。

【0151】さらに、上記実施の形態では、サーバ100で、権利管理の他、コンテンツ配信、課金等をまとめて管理したが、コンテンツ配信や、課金等の機能を別個

に形成するように構成してもよい。

【0152】

【発明の効果】以上の説明から明らかなように、本発明に係るコンテンツ利用管理システムによれば、サーバ装置のライセンスチケット発行手段は前記ユーザからの要求に基づいて、当該ユーザが所有する利用権限の一部を示す権利情報であるライセンスチケットを生成し、前記端末装置に送信する。また、端末装置のコンテンツ利用制御手段は受信されたライセンスチケットが示す利用権限に従って、前記コンテンツの利用を制御する。

【0153】このため、端末装置では、ユーザが所有する全ての利用権限を管理する必要はなく、ライセンスチケットが示すユーザの一部の利用権限を管理するだけでコンテンツの利用を制御でき、端末装置の管理負担を大幅に軽減することができる。また、サーバ装置は、ライセンスチケットの発行に併せて各端末装置でのコンテンツの利用状況を把握することができ、端末装置でコンテンツのコピーなどが行われた場合でも、サーバ装置にコピー許可の問い合わせを行うことで何時どのような媒体にコピーされたかを検知することができ、コンテンツの追跡が可能になる。また、サーバ装置でユーザが所有する利用権限を保持しているので、端末装置の蓄積手段（HDD）がクラッシュした時でも、ユーザの利用条件などを容易に復旧でき、また、コンテンツの利用条件の再生回数を自動的に+1する、と云うようなサービスを実施するような利用条件を拡張するサービスや利用条件の追加などの処理が容易に行える。さらに、端末装置のコンテンツ利用制御手段は受信されたライセンスチケットが示す利用権限に従って、前記コンテンツの利用を制御するので、端末装置でのコンテンツ無制限利用を確実に防止することができる。

【0154】したがって、ユーザ端末に負担を掛けずに、サーバが、ユーザ端末でのコンテンツの利用を確実に且つ簡単に制御することができる。

【図面の簡単な説明】

【図1】本実施の形態に係るコンテンツ利用管理システム1の全体の構成を示す図である。

【図2】図1に示されるサーバ100及びユーザ端末200a～200cの構成を示す機能ブロック図である。

【図3】図2に示されるユーザ管理テーブル111の構成例を示す図である。

【図4】図2に示されるユーザ権利情報管理テーブル121の構成例を示す図である。

【図5】図2に示されるライセンス情報の構成例を示す図である。

【図6】コンテンツ情報生成部170により生成されるLTのデータフォーマット構成を示す図である。

【図7】このシステムにおいて、ユーザがコンテンツを購入する場合のユーザ端末200a及びサーバ100でそれぞれ行われる処理を示すフローチャートである。

【図8】コンテンツ購入画面（1）を示す図である。

【図9】コンテンツ購入画面（2）を示す図である。

10 【図10】このシステムにおいて、ユーザがコンテンツを利用する場合のユーザ端末200a及びサーバ100でそれぞれ行われる処理を示すフローチャートである。

【図11】利用コンテンツ選択画面を示す図である。

【図12】コンテンツ利用要求画面を示す図である。

【図13】ユーザ端末に配信される切り出し利用条件と、サーバで管理される利用条件の変動との関係を示す図である。

【図14】1回の利用条件と利用時間との関係を示す図である。

20 【図15】このシステムにおいて、コンテンツまたはLTを外部メディアに移動する場合のユーザ端末200aで行われる処理を示すフローチャートである。

【図16】移動コンテンツ選択画面を示す図である。

【図17】従来のデジタルコンテンツ配信システムの構成を示すブロック図である。

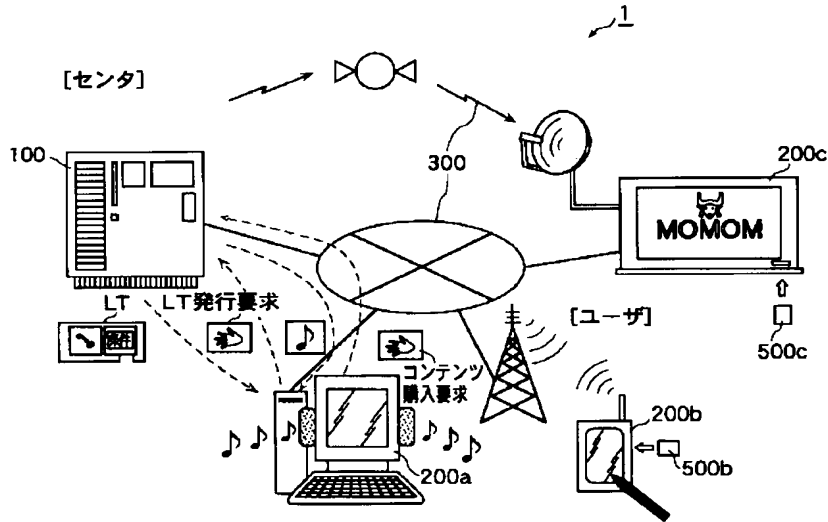
【図18】従来のデジタルコンテンツ配信システムのコンテンツ購入時の処理を示すフローチャートである。

【図19】従来のデジタルコンテンツ配信システムのコンテンツ再生時の処理を示すフローチャートである。

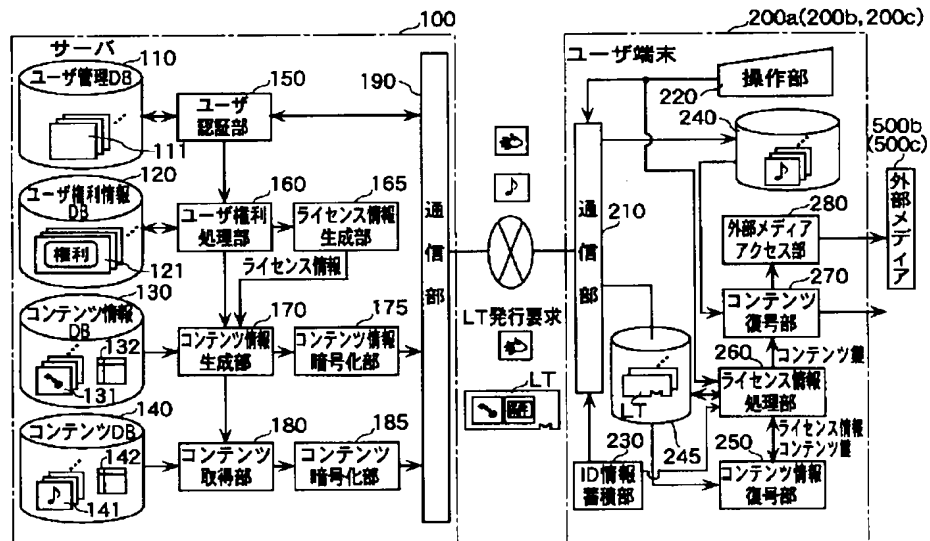
【符号の説明】

1	コンテンツ利用管理システム
100	サーバ
120	ユーザ権利情報DB
121	ユーザ権利情報管理テーブル
160	ユーザ権利処理部
165	ライセンス情報生成部
170	コンテンツ情報生成部
190, 210	通信部
200a～200c	ユーザ端末
260	ライセンス情報処理部
500b, 500c	外部メディア
LT	ライセンスチケット

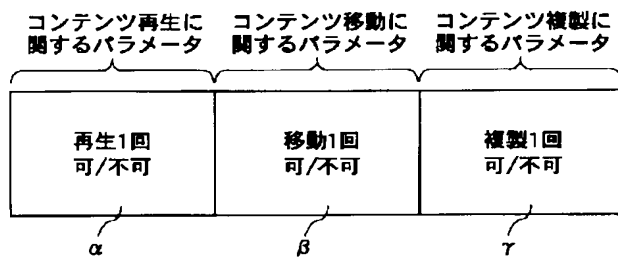
【図1】



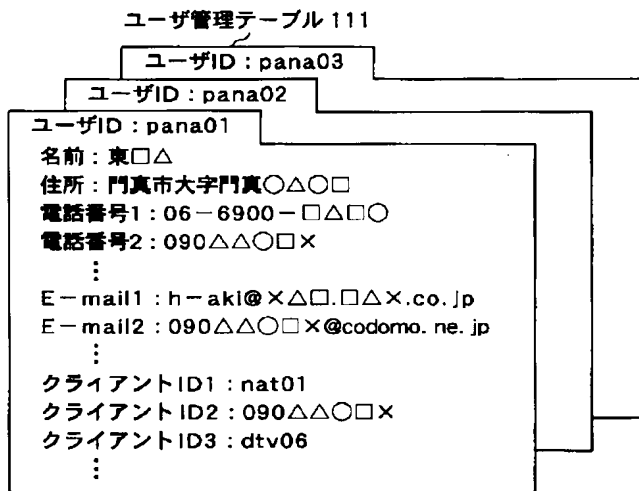
【図2】



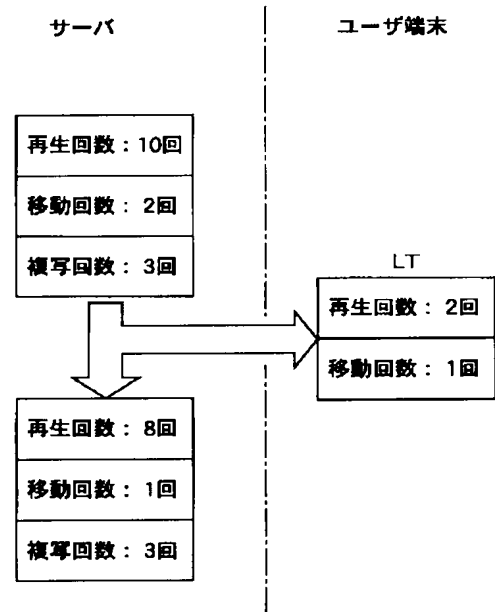
【図5】



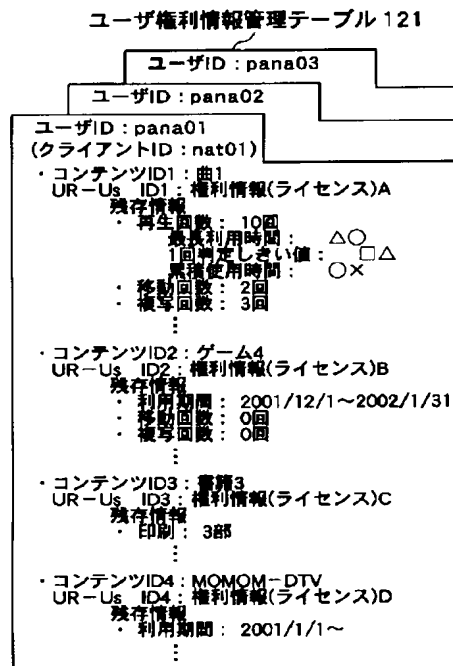
【図3】



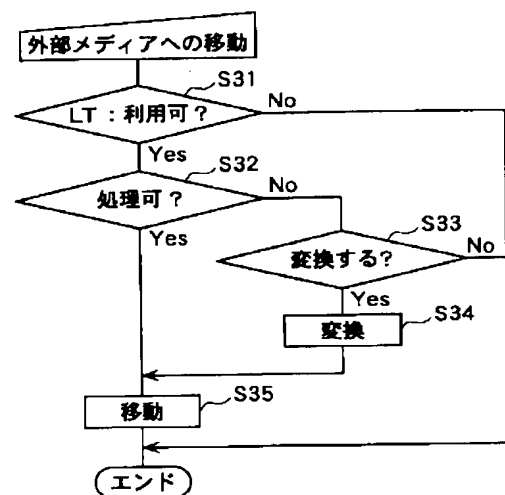
【図13】



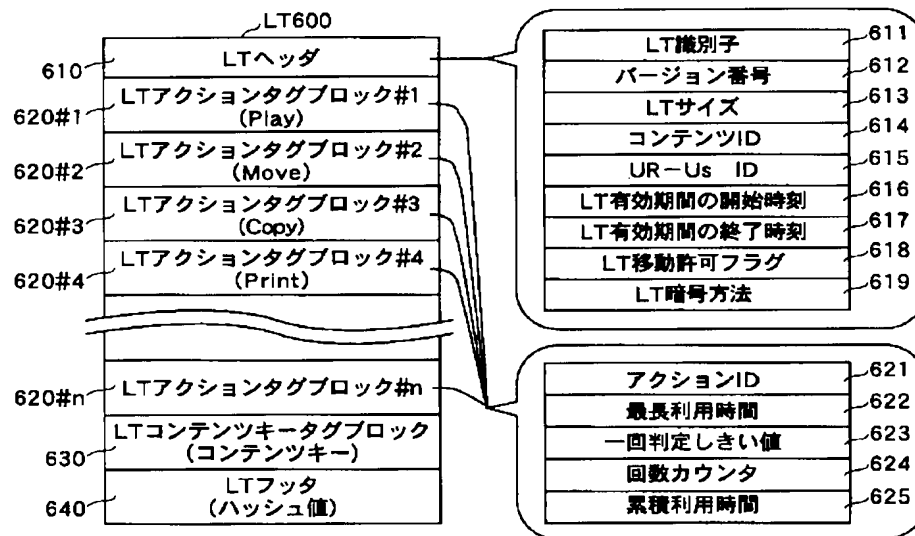
【図4】



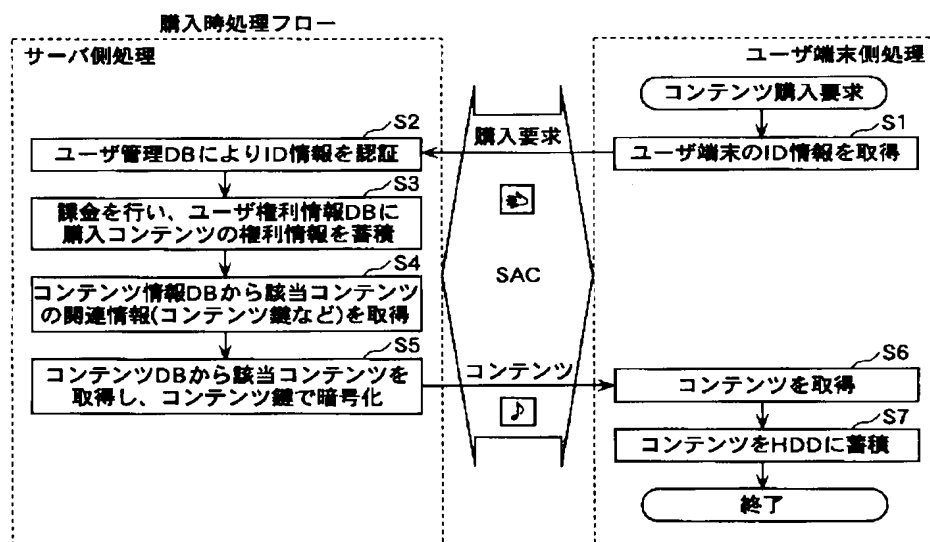
【図15】



【図6】



【図7】



【図8】

コンテンツ購入画面 (1)
購入するコンテンツのジャンルを選択してください。

<input checked="" type="checkbox"/>	音楽
<input type="checkbox"/>	ゲーム
<input type="checkbox"/>	電子書籍
<input type="checkbox"/>	映画
⋮	⋮
<input type="checkbox"/>	有料テレビ番組

次へ
戻る

【図9】

コンテンツ購入画面 (2)

コンテンツID	タイトル	権利情報	販売価格
<input checked="" type="checkbox"/> 曲1	波乗りジョージ	可否情報 利用条件 再生回数 10回 移動回数 2回 複写回数 3回	500円
<input type="checkbox"/> 曲2	アゲハ虫	可否情報 利用条件 利用期間 12/1～12/31 移動回数 禁止 複写回数 禁止	100円
<input type="checkbox"/> 曲3	チュッ!秋パーティ	可否情報 利用条件 再生回数 無制限 移動回数 無制限 複写回数 無制限	1500円

購入
戻る

【図11】

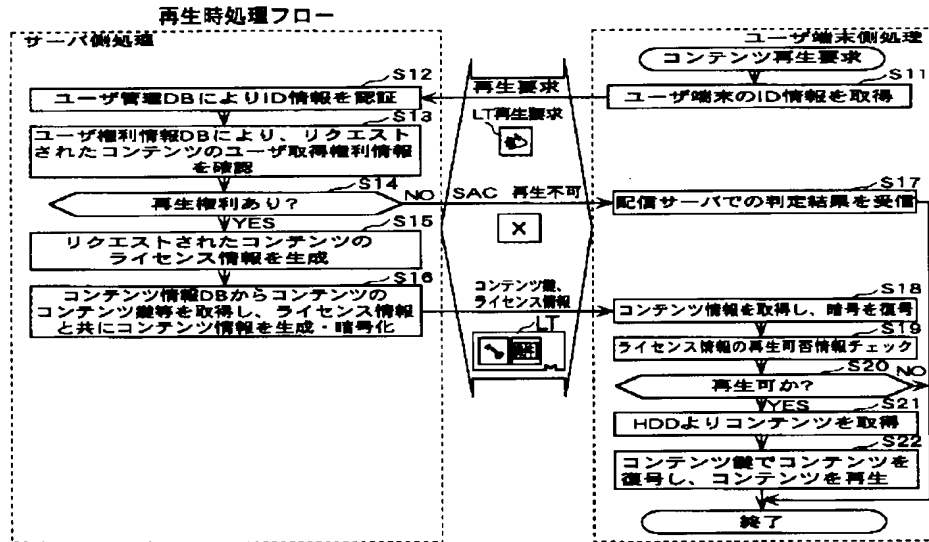
利用コンテンツ選択画面

利用するコンテンツあるいは事前購入するライセンスチケットを1つ選んでください。

<input checked="" type="checkbox"/>	利用要求するコンテンツID 曲1	タイトル 波乗りジョージ
<input type="checkbox"/>	利用要求するコンテンツID ゲーム4	タイトル 真・三国夢想2
<input type="checkbox"/>	利用要求するコンテンツID 書籍3	タイトル オン名字
<input type="checkbox"/>	事前購入するライセンスチケット MOMOM-DTV タイトル 全豪オープンレスリング	

次へ
戻る

【図10】



【図12】

コンテンツ利用要求画面

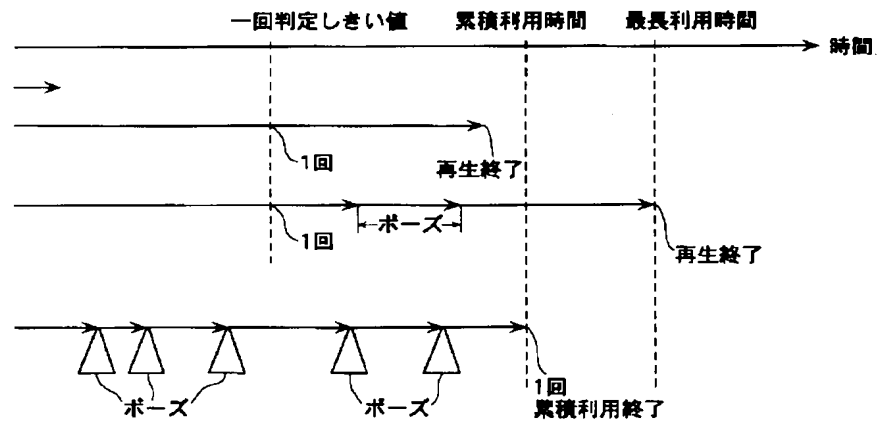
利用要求するコンテンツID 曲1

タイトル 波乗りジョージ

要求内容

<input checked="" type="checkbox"/>	再生	<input type="text" value="2"/>	回
<input checked="" type="checkbox"/>	移動	<input type="text" value="1"/>	回
<input type="checkbox"/>	複写	<input type="text"/>	回

【図14】



【図16】

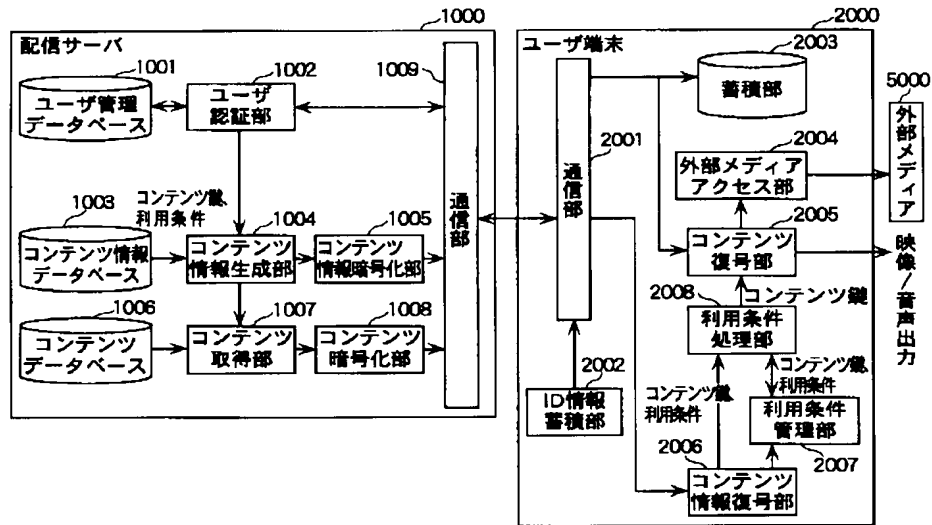
移動コンテンツ選択画面

移動するコンテンツあるいはライセンスチケットを1つ選んでください。

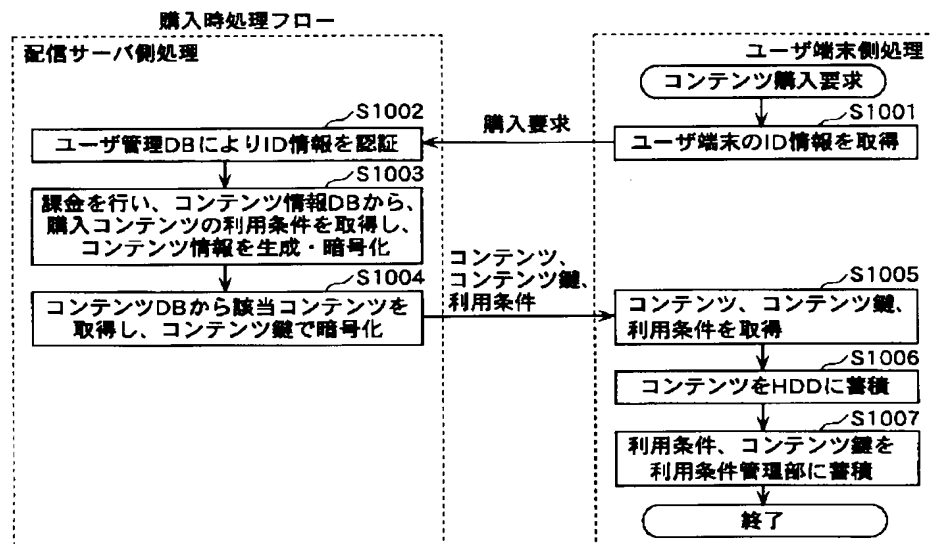
<input checked="" type="checkbox"/> 移動するコンテンツID 曲1	タイトル 波乗りジョージ
<input type="checkbox"/> 移動するコンテンツID ゲーム4	タイトル 裏・三国夢想2
<input type="checkbox"/> 移動するコンテンツID 書籍3	タイトル オン名字
<input type="checkbox"/> 移動するライセンスチケット MOMOM-DTV	タイトル 全豪オープンレスリング

決定

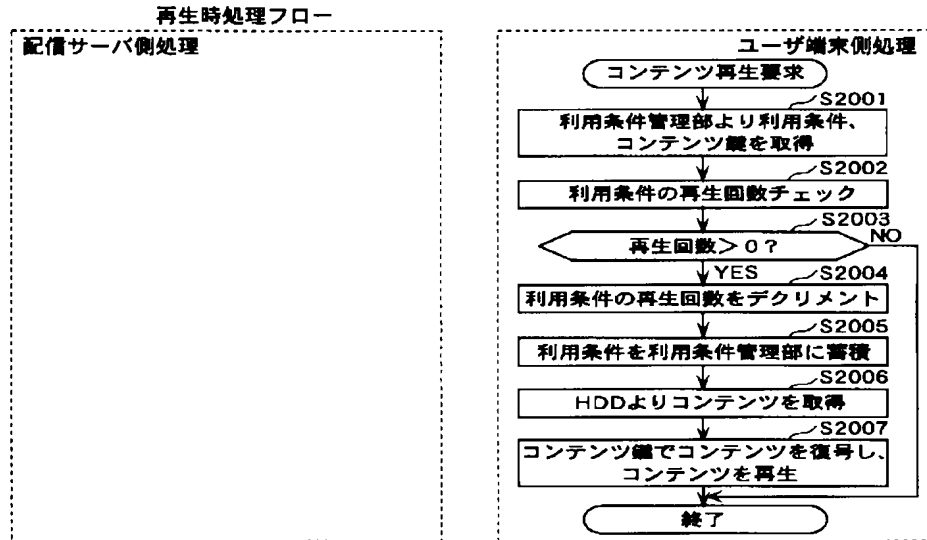
【図17】



【図18】



【図19】



フロントページの続き

(51) Int.Cl. ⁷		識別記号	F I	テマコード (参考)	
H 0 4 N	5/765		H 0 4 N	7/173	6 1 0 Z
	5/91			5/91	P
	7/173	6 1 0			L
(72)発明者	松尾 隆史		(72)発明者	中西 正典	
	大阪府門真市大字門真1006番地 松下電器産業株式会社内			大阪府門真市大字門真1006番地 松下電器産業株式会社内	
(72)発明者	中原 徹		(72)発明者	宮▲崎▼ 雅也	
	大阪府門真市大字門真1006番地 松下電器産業株式会社内			大阪府門真市大字門真1006番地 松下電器産業株式会社内	
(72)発明者	難波 孝彰		(72)発明者	小塚 雅之	
	愛知県名古屋市中区栄2丁目6番1号白川ビル別館5階 株式会社松下電器情報システム名古屋研究所内			大阪府門真市大字門真1006番地 松下電器産業株式会社内	
(72)発明者	後藤 吉正		F ターム(参考)	5B017 AA06 BA06 CA15	
	大阪府門真市大字門真1006番地 松下電器産業株式会社内			5B085 AE29 BA06 BE07 BG03 BG07	
				5C053 FA13 FA23 GB06 JA21 LA15	
				5C064 BA07 BB02 BC01 BC06 BC17	
				BC18 BC22 BC25 BD02 BD03	
				BD08 BD13 CA14 CB01 CC04	